



PHILIPS

Security Testing Report

IGT Solutions

CAD GHS 1.0.1

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Table of Contents

| | |
|---|----|
| Document Version Control..... | 4 |
| Document History | 4 |
| Distribution List | 5 |
| 1. Definitions & Abbreviations | 6 |
| 2. System Details & Architecture..... | 8 |
| 3. Scope | 9 |
| Not in Scope | 11 |
| 4. Executive Summary | 12 |
| 5. Vulnerability Summary | 14 |
| 6. Observations..... | 16 |
| 7. Detailed Vulnerability Report..... | 18 |
| 7.1 Webapp/WebServices: Account Takeover: Privilege Escalation..... | 18 |
| 7.2 Webapp: Functionality Misuse Due to Missing Authentication..... | 22 |
| 7.3 Webapp: Modifiable Redirect URI Parameter..... | 29 |
| 7.4 Webapp: Rate Limiting Not Implemented | 35 |
| 7.5 Webapp: Client Side Validation Bypass..... | 43 |
| 7.6 Webapp: Weak SSL/TLS configuration | 48 |
| 7.7 Webapp/WebServices: Improper Session Management | 55 |
| 7.8 Webapp: Lack of Authorization | 62 |
| 7.9 Webapp/WebServices: Sensitive Information in URL | 65 |
| 7.10 Webapp: Misconfigured CORS | 70 |
| 7.11 Webapp/WebServices: HTTPS Fallback Allowed..... | 74 |
| 7.12 Webapp/WebServices: Server Banner Disclosure | 79 |
| 7.13 Webapp/WebServices: Improper Error Handling | 83 |
| 7.14 Webapp: Missing Security Headers..... | 87 |
| 7.15 Webapp: Sensitive file exposed | 90 |
| 7.16 Webapp: User Email Enumeration | 92 |
| 7.17 WebServices: Misconfigured CORS | 95 |
| 8. Tools Used | 98 |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).





| | |
|---|----|
| 9. Automated Tool Report..... | 98 |
| 10. Manual Test Reports and Test Case Execution | 98 |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Document Version Control

| | | |
|---|------------------------|---------------------------|
| Name of the document : CAD GHS 1.0.1 Security Testing Report | | |
| Version: 6.0 | Intake ID: | 2695 |
| Document Definition: This document highlights the vulnerabilities currently existing in the application under scope. It also documents possible actions to be taken to reduce/eliminate the vulnerabilities. | Document ID: | PRHC/C40/SVN/80639 |
| Author: Sai Praneetha Bhaskaruni, Harshal Kukade | Effective Date: | 27 July 2023 |
| Reviewed by: Chaitra N Shivayogimath | | |

Document History

| Version | Date | Author | Section | Changes |
|---------|---------------|--|----------|--------------------------------------|
| 0.1 | 16 Dec 2022 | Chaitra N Shivayogimath | Complete | Initial Draft |
| 1.0 | 19 Dec 2022 | Ashwin K K | Complete | Final Review |
| 1.1 | 10 Feb 2023 | Chaitra N Shivayogimath | Complete | Retest and Reporting |
| 2.0 | 13 Feb 2023 | Ashwin K K | Complete | Final Review |
| 2.1 | 19 April 2023 | Chaitra N Shivayogimath & Meba Meria Jacob | Complete | Initial Draft |
| 3.0 | 19 April 2023 | Shabana Bagum | Complete | Final Review |
| 3.1 | 27 April 2023 | Meba Meria Jacob | Complete | Revalidation of 7.3, 7.5, 7.8 & 7.10 |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | | | | |
|------------|----------------------|---|-----------------|--------------------------------------|
| 4.0 | 27 April 2023 | Chaitra N Shivayogimath | Complete | Final Review |
| 4.1 | 02 May 2023 | Meba Meria Jacob | Complete | Revalidation of 7.3 & 7.8 |
| 5.0 | 02 May 2023 | Chaitra N Shivayogimath | Complete | Final Review |
| 5.1 | 05 May 2023 | Meba Meria Jacob | Complete | Revalidation of 7.4 &7.5 |
| 5.2 | 05 May 2023 | Chaitra N Shivayogimath | Complete | Final Review |
| 5.3 | 24 July 2023 | Harshal Kukade, Sai Praneetha Bhaskaruni | Complete | Addition & Review |
| 6.0 | 27 July 2023 | Chaitra N Shivayogimath | Complete | Final Review |

Distribution List

| User/Department/Stakeholder | E-Mail ID |
|------------------------------|--|
| Project Owner and PSO | SakethM.Jain@philips.com ; Chandrashekhar.Natarajan@philips.com ; Priya.Vijayachandran@philips.com ; anand.kumaraiswal@philips.com sreenath.kooloth@philips.com karthik.srinivasan@philips.com |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



1. Definitions & Abbreviations

| Term | Explanation |
|------|-------------------------------|
| SCoE | Security Center of Excellence |
| TLS | Transport Layer Security |
| SSL | Secure Socket Layer |
| XSS | Cross Site Scripting |
| CORS | Cross Origin Resource Sharing |
| CAD | Coronary Artery Disease |
| NBX | New Business Creation |
| B2B | Business To Business |
| B2C | Business to Consumer |
| GHS | Guided Health Services |

The severity of every vulnerability has been calculated by using industry standard **Common Vulnerability Scoring System (CVSS)** used for assessing the severity of computer system vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score (Scores range from 0 to 10, with 10 being the most severe) reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organization properly assess and prioritize their vulnerability management processes.

| The severity rating for the numerical values are mapped below | |
|---|------------|
| None | 0.0 |
| Low | 0.1 - 3.9 |
| Medium | 4.0 - 6.9 |
| High | 7.0 - 8.9 |
| Critical | 9.0 - 10.0 |

The **Severity** and **CVSS vector** of each vulnerability is calculated using the CVSS V3 **Base Score Metrics** Calculator located [here](#). Vulnerabilities identified during security assessment are classified into standardized categories. Refer following table for more information:

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



| Categories for vulnerability classification | |
|---|----------------------|
| Web application security assessment | OWASP Top Ten - 2021 |
| Mobile application security assessment | OWASP Top Ten - 2016 |
| IoT/Hardware security assessment | OWASP Top Ten – 2014 |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



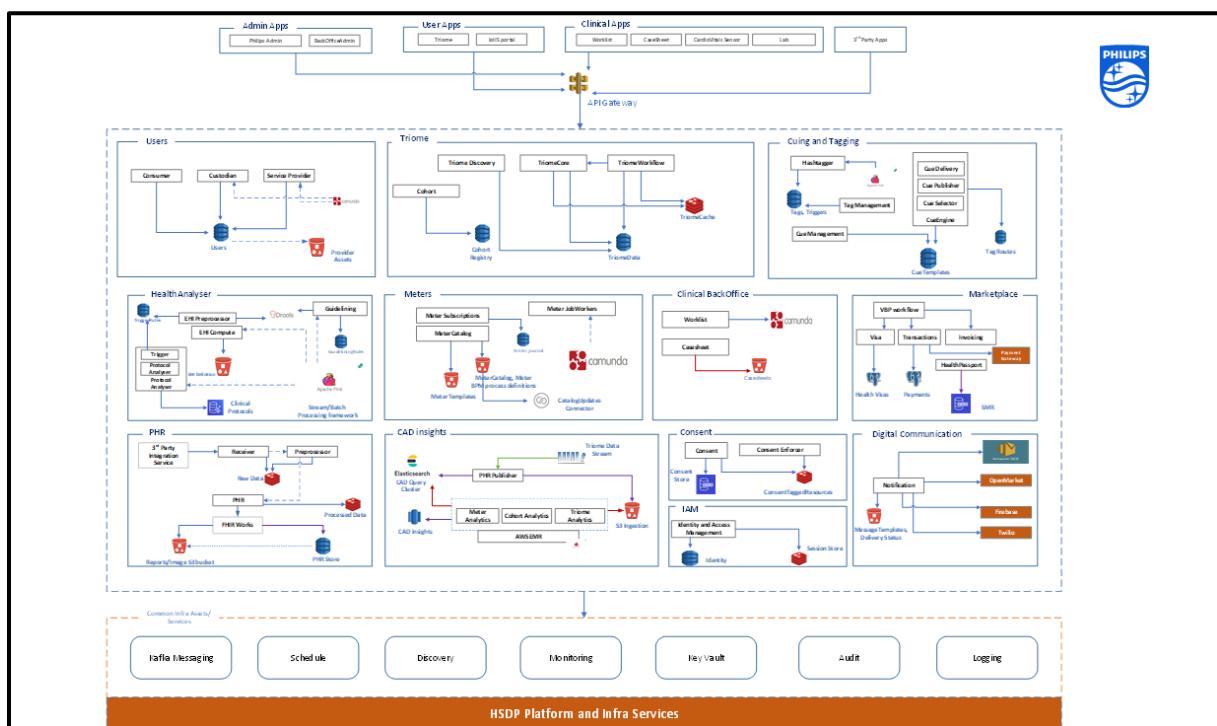
2. System Details & Architecture

A Conceptual Overview of CAD GHS Web application:

- Engages consumers towards their cardiac health through monitoring, forecasting and guideline
 - A proactive health services marketplace (B2C and B2B) backed by outcome-based services (meters)
 - Post MVP, expand the solution to assurance services for large cohorts based on protocol-based clinical guidance and AI-driven differential diagnosis

Test Environment: Validation

Architecture Diagram:



PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



3. Scope

The scope of this security assessment is to perform **Grey-Box** security testing to find security threats that may come from a malicious outsider or insider user of the **CAD GHS 1.0.1**. Security testing on **Web application/Web Services** of the **CAD GHS 1.0.1** is performed.

The following list includes some examples of major activities performed during the assessment:

Web Application/Web Services:

1. Retest of previous **Web** findings & fixes:
 - Missing Security Headers.
 - Server Banner Disclosure.
 - OTP Rate Limit (IAM) - login page redirection.
 - Reuse of old OTP within 4minutes.
 2. Fresh test of 2 New **Web Services/API** Endpoints: View Report Feature
 1. GET: <BaseUrl>/engagement/report
 - Params
 - reportStartDate=2023-07-12T17:17:51Z
 - reportEndDate=2023-07-13T11:02:49Z
 - reportType=BEATS
 - userId=<UUID>
 2. POST: <BaseUrl>/engagement/report
 - Payload
 - {
 - "assessmentRecordIds": [
 - ,
 - "userId": "",
 - "requestId": "",
 - "reportStartDate": "",
 - "reportEndDate": ""
- Crawl through complete scope of the web application/service space and identify for any unauthenticated URL or directory.
 - Check for all input injection-based attacks across all the possible entry fields in Web API.
 - Exploiting any known component vulnerability or service misconfiguration.
 - Reviewing the transport layer security implemented.

Follow "[Test case execution](#)" section to get the detailed about test cases.



The test scope for this release is explained in the below table:

| Start Date | End Date | Applications/Devices/IP's/URL's |
|--------------|--------------|---|
| 19-July-2023 | 24-July-2023 | <p>CAD GHS:</p> <p>Web Application:</p> <ul style="list-style-type: none">• URLs: https://cad-consumer-app-int.us-east.philips-healthsuite.com/• Environment: Test• Version: 1.0.1• User Role: Consumer, Custodian, Admin <p>Web Services:</p> <ul style="list-style-type: none">• URL: https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report• Environment: Test• Version: 1.0.1• User Role: Consumer, Custodian, Admin |

CAD GHS is a web application which can be accessed via Mobile Web Browser.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Not in Scope

Below mentioned items are out of scope for the current security assessment:

- Source Code Review
- Network Testing
- AI Component
- Complete Web Application Testing (There are few features not developed yet)

Note: The environment provided was not stable. We have covered the testing of **CAD GHS 1.0.1** in the environment provided and the results are valid if the same environment is replicated. Re-run the tests if a new propagation of the environment is made.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



4. Executive Summary

Security Center of Excellence team engaged in activity to conduct security assessment of **CAD GHS 1.0.1** which included **Web Application/Web Service Testing** in scope. The purpose of the engagement was to evaluate the security of the **CAD GHS 1.0.1** against industry best practice criteria.

Note: Application is in nascent stage and features were not stable during testing phase.

Revalidation of previous findings carried out on 24th July, 2023 and updated the report accordingly. Identified 2 new vulnerabilities.

Note: Only highlights of important vulnerabilities are described below. Please refer 'Vulnerability Summary' section for complete detailed list of vulnerabilities.

During the security assessment of the product, security issues in the below area is found:

- Weak TLS/SSL Configuration
- Improper Session Management
- Sensitive Information in URL
- HTTPS Fallback Allowed
- Improper Error Handling
- Missing Security Headers
- Sensitive file exposed
- User Email Enumeration

During the security assessment of the product, security issues in the below areas were not found:

- CSRF Attacks
- Input Validation

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



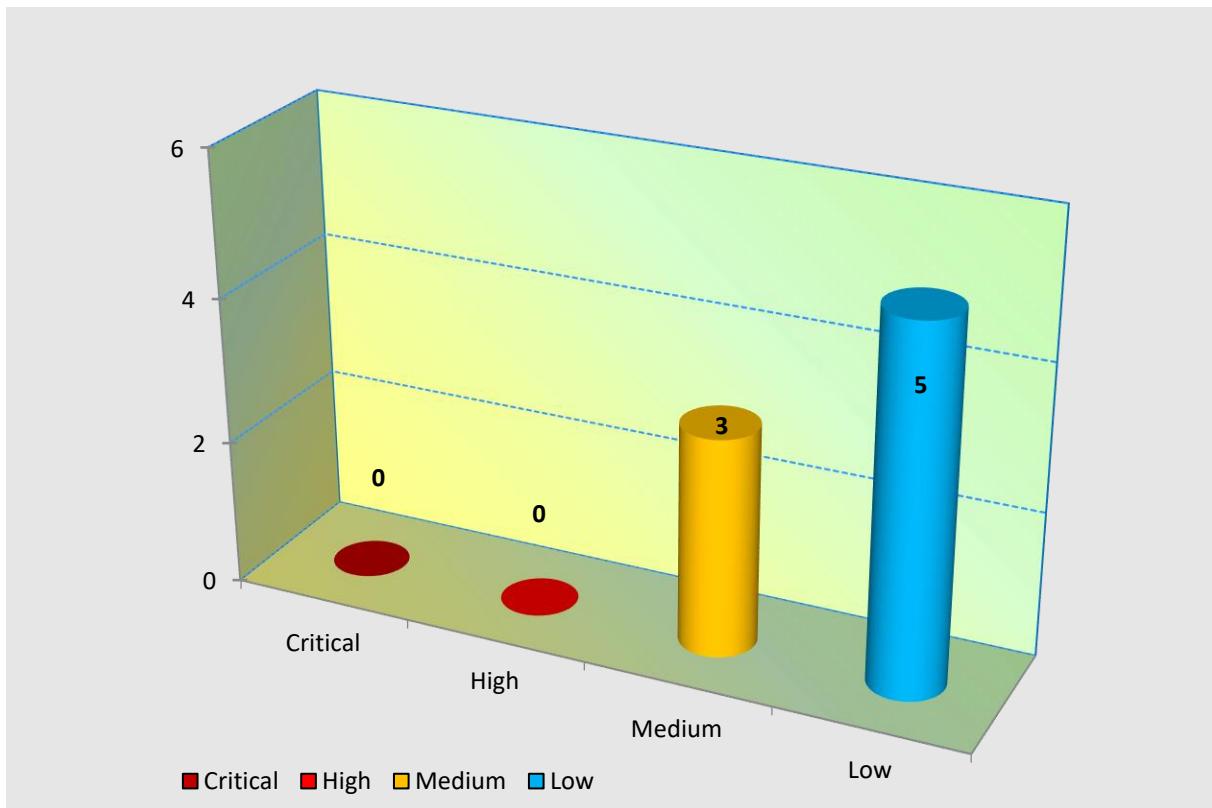
Printed copies are uncontrolled unless authenticated.



VULNERABILITY SUMMARY CHART

The graph below shows a summary of the number of vulnerabilities and their severities.

Note: The vulnerabilities mentioned in this report are technical vulnerabilities only. The Product Security Risk Assessment would report the business risks associated with these vulnerabilities.



Note: - 1 informational finding not included in Chart

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



5. Vulnerability Summary

The Findings and vulnerabilities from the assessment are tabulated below

| Finding No. | Vulnerability Title | Technical Risk | Impacted Area | CVE ID* | Status (02 May 2023) | Revalidation Status (05/May/2023) | Revalidation Status (24/July/2023) |
|-------------|--|----------------|--------------------|---------|----------------------|-----------------------------------|------------------------------------|
| 86078 | Account Takeover: Privilege Escalation | High | Webapp/ WebService | NA | Closed | Closed | Closed |
| 82881 | Functionality Misuse Due to Missing Authentication | Medium | Webapp | NA | Closed | Closed | Closed |
| 82752 | Modifiable Redirect URI Parameter | Medium | Webapp | NA | Closed | Closed | Closed |
| 82899 | Rate Limiting Not Implemented | Medium | Webapp | NA | Open | Closed | Closed |
| 82900 | Client Side Validation Bypass | Informational | Webapp | NA | Open | Open | Closed |
| 84070 | Weak TLS/SSL Configuration | Medium | Webapp | NA | Open | Open | Open |
| 85889 | Improper Session Management | Medium | Webapp/ WebService | NA | Open | Open | Open |
| 86079 | Lack of Authorization | Medium | Webapp | NA | Closed | Closed | Closed |
| 85892 | Sensitive Information in URL | Low | Webapp/ WebService | NA | Open | Open | Open |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | | | | | | | |
|-------|--------------------------|--------|-----------------------|----|--------|--------|--------|
| 82753 | Misconfigured CORS | Low | Webapp | NA | Closed | Closed | Closed |
| 82916 | HTTPS Fallback Allowed | Low | Webapp/ WebService | NA | Open | Open | Open |
| 82886 | Server Banner Disclosure | Low | Webapp/ WebService | NA | Open | Open | Closed |
| 85890 | Improper Error Handling | Low | Webapp/ WebService | NA | Open | Open | Open |
| 86080 | Missing Security Headers | Low | Webapp | NA | Open | Open | Open |
| 87720 | Sensitive file exposed | Medium | Webapp | NA | NA | NA | Open |
| 87721 | User Email Enumeration | Low | Webapp | NA | NA | NA | Open |
| 87725 | Misconfigured CORS | Low | WebServices | NA | NA | NA | Closed |

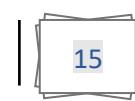
*CVE ID are mentioned for the vulnerabilities which has a known external CVE.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



6. Observations

Below mentioned observations are not considered as Vulnerability but informative to the business.

Observations which shows good implementation or best practice identified:

1. SCoE observed that strong input validation was in place for the user input.

Observations which shows weak implementation are:

1. It is observed that the oauth session cookie has certain misconfigurations: It is recommended to not scope the cookie to parent domain and secure flag should be set to the cookie.
 - Cookie is scoped to parent domain
 - Cookie expires after 1 week, which is very long duration.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).





- It was observed that the application does not properly invalidate a user's session on the server after the user initiates logout. User sessions remain active on the server, and any requests submitted including the user's session identifier will execute successfully, as though the user had made those requests. However, since the JWT token expires only after 20 min, the issue is kept in the observation.

Refer Video POC

3. It is observed that for some API endpoints, HTTP methods are not properly defined.

HEAD Method allowed

HTTP/s supported methods shown in server response

PHILIPS SCOF

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



7. Detailed Vulnerability Report

7.1 Webapp/WebServices: Account Takeover: Privilege Escalation

| | |
|---------------------------------|--|
| Vulnerability Title | Account Takeover: Privilege Escalation |
| Vulnerability Category | A1 Broken Access Control |
| Severity | High |
| CVSS V3 Calculation | CVSS Base Score: 8.8 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| Description | <p>Vulnerability Description: During the security assessment it was observed that a custodian user will be able to login as an admin user by just changing the login_hint:EMAIL: (or even PHONENUMBER) parameter after providing the OTP of that user.</p> <p>Retest as of 18-Apr-2023: The issue is fixed.</p> <p>Retest as of 24-July-2023: The issue is fixed.</p> <p>Exploitability Rational: An attacker needs to know the admin username(emailID) and be any valid user for the application.</p> <p>Impact Rational: Complete account takeover of the admin user can be done.</p> |
| Affected Systems/IP Address/URL | https://cad-consumer-app-int.us-east.philips-healthsuite.com/signin WebService Endpoint: https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report |
| Recommendation | It is recommended to validate the Email parameter in the /oauth/authorize? LoginHint parameter. This parameter should not be passed as a part of the GET request and it needs to be mapped to the code verifier/code challenge/session id. |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | |
|--------|--------|
| Status | Closed |
|--------|--------|

Supportive Evidence:

Please refer the video POC:

[AccountTakeover.wmv](#)

Retest Evidence as of 18 Apr 2023:

https://docs.philips.com/v/g/personal/chaitran_shivayogimath_philips_com/EScEBADh32NEocbA2RAUSXABKRfrqvORwvx16OveKDNCZQ?e=WJdBiH

[S_AccountTakeover_2.wmv](#)

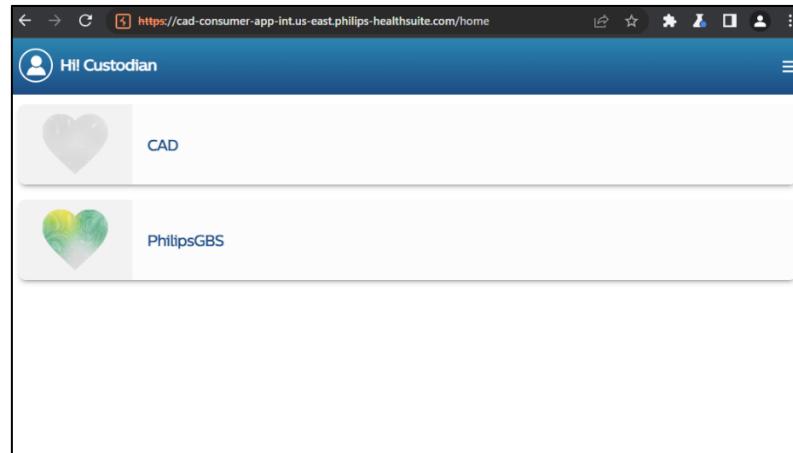
Retest Evidence as of 24 July 2023:

Case 1: WebApp

```

Send | Cancel | < | > | Follow redirection | Target: https://cad-api-gateway-int.us-east.philips-healthsuite.com | HTTP/1
Request | Response
Pretty Raw Hex | Pretty Raw Hex Render
1 POST /oauth/login HTTP/1.1
2 Host: cad-api-gateway-int.us-east.philips-healthsuite.com
3 Cookie: SESSION=2ceee2f7-ae44-4210-85e7-ec814e43cb89
4 Content-Length: 268
5 Cache-Control: max-age=0
6 Sec-Ch-Ua:
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: ""
9 Upgrade-Insecure-Requests: 1
0 Origin: null
1 Content-Type: application/x-www-form-urlencoded
2 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36
3 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
4 Accept-Charset: utf-8,*application/signed-exchange;v=b3;q=0.7
5 Sec-Fetch-Site: same-origin
6 Sec-Fetch-Mode: navigate
7 Sec-Fetch-User: ?1
8 Sec-Fetch-Dest: document
9 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
0 Connection: close
1
2 type=EMAIL&username=cad-security140grr.laspassword=111111&login_hint=
EMAIL%3Acad-security140grr.lascode_challenge=
G5wiypfmD5xNCVWjX5M7gdsyBmao7Qx7f01d5342mZB%code_challenge_method=SHA256
redirect_uri=https%3A%2F%2Fcad-consumer-app-int.us-east.philips-healthsuite.com

```



Test Evidence as of 24 July 2023:

Case 2: WebServices

Request

```

Send Cancel < > Target: https://cad-api-gateway-int.us-east.philips-healthsuite.com
Pretty Raw ▾ Actions ▾
1. GET /engagement/report3/reportStartDate=2023-07-14T14:22:30Z/reportEndDate=2023-07-14T14:22:30Z&reportType=BEAT
2. Access-Control-Allow-Credentials: true
3. Access-Control-Allow-Origin: https://cad-consumer-app-int.us-east.philips-healthsuite.com
4. Access-Control-Expose-Header: Accept,Accept-Encoding,Connection,Content-Length,Keep-Alive,Location,Set-Cookie,User-Agent
5. Content-Security-Policy: default-src 'self' *.philips-healthsuite.com
6. Content-Type: application/json
7. Date: Tue, 18 Jul 2023 05:31:36 GMT
8. Strict-Transport-Security: max-age=63072000; includeSubDomains
9. X-Envoy-Upstream-Service-Time: 31
10. X-Vcap-Request-Id: eeab2579-8d02-401b-788a-11cc54508f31
11. Content-Length: 3240
12. Connection: Close
  
```

Response

```

Pretty Raw Render ▾ Actions ▾
1. HTTP/1.1 200 OK
2. Access-Control-Allow-Credentials: true
3. Access-Control-Allow-Origin: https://cad-consumer-app-int.us-east.philips-healthsuite.com
4. Access-Control-Expose-Header: Accept,Accept-Encoding,Connection,Content-Length,Keep-Alive,Location,Set-Cookie,User-Agent
5. Content-Security-Policy: default-src 'self' *.philips-healthsuite.com
6. Content-Type: application/json
7. Date: Tue, 18 Jul 2023 05:31:36 GMT
8. Strict-Transport-Security: max-age=63072000; includeSubDomains
9. X-Envoy-Upstream-Service-Time: 31
10. X-Vcap-Request-Id: eeab2579-8d02-401b-788a-11cc54508f31
11. Content-Length: 3240
12. Connection: Close
  
```

INSPECTOR

- Query Parameters (4)
- Body Parameters (0)
- Request Cookies (1)
- Request Headers (15)
- Response Headers (13)

Activate Windows

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).





By replacing A's user id with B's user id, we are able to see the B's data.

Case 2:

Retest Evidence as of 28 July 2023:

User id is not visible. Not able to modify the same. Issue is fixed

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



7.2 Webapp: Functionality Misuse Due to Missing Authentication

| | |
|---------------------------------|--|
| Vulnerability Title | Functionality Misuse Due to Missing Authentication |
| Vulnerability Category | A7 Identification and Authentication Failures |
| Severity | Medium |
| CVSS V3 Calculation | CVSS Base Score: 5.9 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N |
| Description | <p>Vulnerability Description: Upon Subscribing when we start Day 1, We get a URL to scan the Vitals of the patient. This URL can be accessed without any authentication and the vitals can be scanned. Upon clicking on save we are redirected to Login page. When we check for resume scan in the logged in Session the results would have already been submitted and we get to questionnaires part. We have observed that there is no JWT passed for this request.</p> <p>Retest Status: The issue is not fixed. The severity is reduced to Medium as the id and code in the URL expires in 5 mins.</p> <p>Retest Status(17/April/2023): Proper Authentication has been implemented. Hence the issue is CLOSED.</p> <p>Retest as of 24-July-2023: The issue is fixed.</p> <p>Exploitability Rational: Anyone having access to the scan URL can exploit this vulnerability.</p> <p>Impact Rational: Anyone can scan and use the application functionality even without authentication. The scan results gets saved even without authentication.</p> |
| Affected Systems/IP Address/URL | https://cad-cardiovital-app-int.us-east.philips-healthsuite.com/?id=U2FsdGVkX1+zlu8S3Cgkt4iZlpUrn42ACWZz4usKIVKVFAAs/3WiD2e6074a/Ylzl9beNilENs4oShjRVU0ymc6mvpRah8FA7QglOTDetKfljxxIXIMUbR88pxx71pQ7pivMPD1H4dXFQl8ij/mNJ1cr6R+pCrKlx5+fDobJoHNe93xjb9Qup9QMWEmQabGJ6wVDI4etgtmrQsfKOMzaNKEj20KUzN9vjVp+HbM4qDusTVsJFhVqV9WECKcl2wJnDrqoSxohIP2E1qNWudIFjbH6DED4szrj8p6J6gVkbFYy7+yKnUaimpbpz3Y0bbwVZRkUYeSOMwvleFg419vwkNLXCZIDLZyMzTnt5VxEw8DQGnFzwmcZn283x0qbAAJNmVphRkTd/8gPtnyvTm9AmkKueQGTfQPCqqIG72gi |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



| | |
|-----------------------|---|
| | <p>KW3zKrzSj/aKroUIUB6EeJaVsFum0/tNxTMjxwMdEAhfscUWzwXBm1hRQ+iElSnqWjxzGkBK5EASf5XFw5ApZ70G/5esQ8Yx4YtzTlHs5h8p1Z3eg8MEeaqL5oNnPw3PHImqSRy71s0iSOHk+ZDvUV01XLj6T159qzX9pzsXgJ0a/OvbWJHmbserIX+7EjuLQFc9NWX6PIESLQyoilZu/D/Ge/tgRPTYZXYHWF5JENMIwLLig9eTrSUqNdtAZ8z4jE6rbGEPgI0TTsruQTJ81fsAgK1+WgycGXCbhmwaLCsgB1YBWknhhmz8aoxktmkhW1vE+0w0JvbBvd4HXA54vQ2Mp9FLAanKH4zWwrEumYrivQ0ZiPqyk/VhXB+dUY7faCZ5exsEHlvg8B5tSwVgcmKOWEDVBDhe37K+JO27seid03V1RTjjMBg2HtU81OehGIKimSJ0YYxc7i1AibrwDifx6H7cSdUY8p+/XvcO2+qwll8ZvmnzVLkSNI3G0I/9u83JYpZeZ4I35W0aEJLqCcLCSyJvHWKwWOWTCAj2d+32TeBQlbSZ8mrYpXAe3uRR8Jntvmi0nT0CIF2gEsP9AEZ96WTnFk3AB37FxIqVh5nSEFyxaEJGPD5QR0m116RKLjep0ZGG4eEqvwfVESRzzCXEoSfPJ5gMMeRLZFmrMewT8ONClwyVI0QhiEHjLRvNd1ek9udOH44cOMwllsPMRmmfyI2QuYJJG/9Vtk/aeN5SKZzu6HfkWvB2o7GeLnuT2rj6mz3lwIqz8HDvTRYq/jNvbF37V4+/WfhzpntC/XBB0nT4cftqVx0UPvNp26XFd/wsLa4IskCUW7UOMNYQ7ITNiSzzYm1D8cENVy2h59muROk1hfb4mlQkej9Jp8oK/HnZrh9zXghBdJDz6mLHlbFxuWeMmd5HoiNAa5gxO+sOGzdKYhHu7M/yPZOhi3jWulngZpKLjPdhJZ2XloKL2CVXrwhh4WqtDfadEZIFpCO3KEVi1RIFoMLrxbWAo6zf9GBib9WkXiK+m5CiE2jQvXlyJWFd+PZSxPBe5is0GLEvaQTo0GO/MEP1Xq8zreaSgmEyQUrCniN/RPwvc3fl7amclNLBJBN+2/bLcfdbz5NEplUu3BUhiF2ICgThYClq1FM5Wqu2yQxo5lgJlcUtzm3gpg6yAbNAcSKM7R/FvfgHi1mvEM/1lyEnrgozBXAU2n+Oil34dqIMFZXzULkjr7tedAYd+7E5o8h/eZHRDwumRcWjEgbTROdWqi5Jx7KV+ubrNcEU9c9YhwrlSellj7wa3Z80Fqs3MyygfSprC7FFnXP7A7E1YhMyL7IVA8SmuijtAFALT/B4fWyUD7JL+Rad/7tCYmhne5TE3Ayl030dwkgU4MXPF+askXe3CcTzhLnxGdwUw89GdQFVVJxevbrJ8YADUNohAhJp4kczm1AWHsF7ugME5iHRxXJ3QoSfRFutSq1SdY9D5RDUZBVWfTXDoZTN1us9WJTxxEovnmkARThbOpgZ/11gTnhZ5ExQSb6GgGJ793msowwmipCiLtk4mLn2MB7KVlloycxfL0gA428BF53cw9JOqyVThqoayHO9J3Rup2A0ADq0p925JSHNt+EX2DLdiacZGZJ9KC0j9sW2XyMDMbJ1thxk3+tgT6B5c+Xy0aC0cRs7Eq8Fq9ilANfynLis2mBNzT583LzKXGdfOGfk0IQCT8jQdyMU+kL</p> <p>https://cad-consumer-app-int.us-east.philips-healthsuite.com/?code=8545169a917ede5f8b84bf03b1ef3be556a2b6917c824c6346&login_hint=9916337921</p> |
| Recommendation | Authentication should be enforced for all resources that require any form of restriction from users. There should be session handled for this feature |
| Status | Closed |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



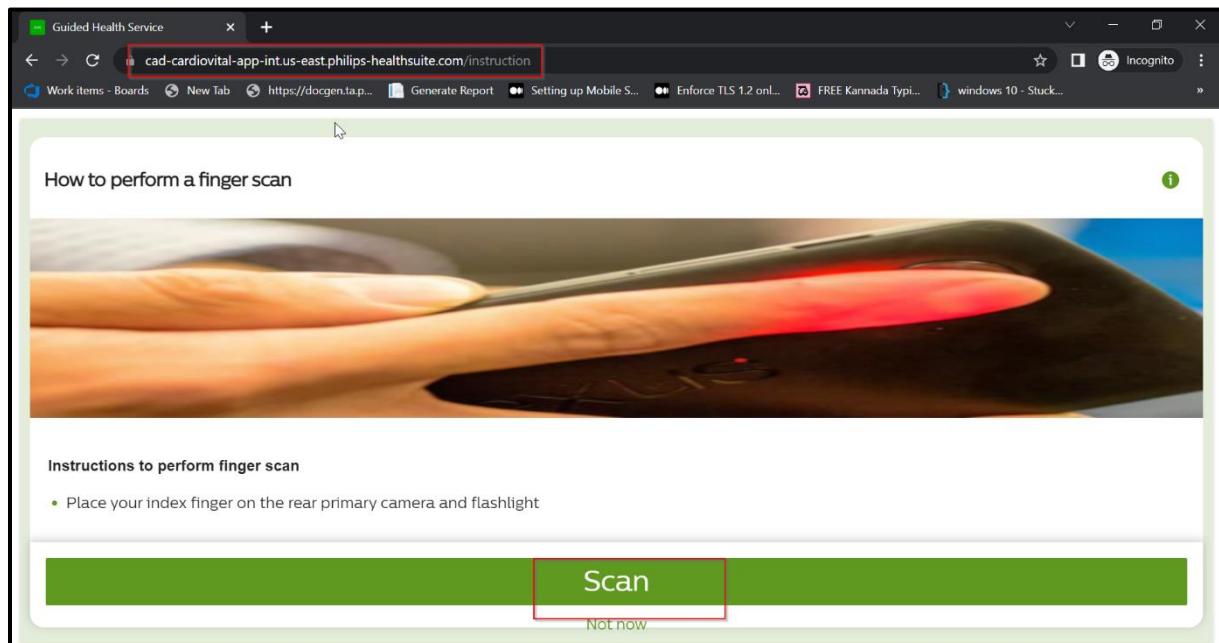
Steps to Reproduce

Refer the video POC:

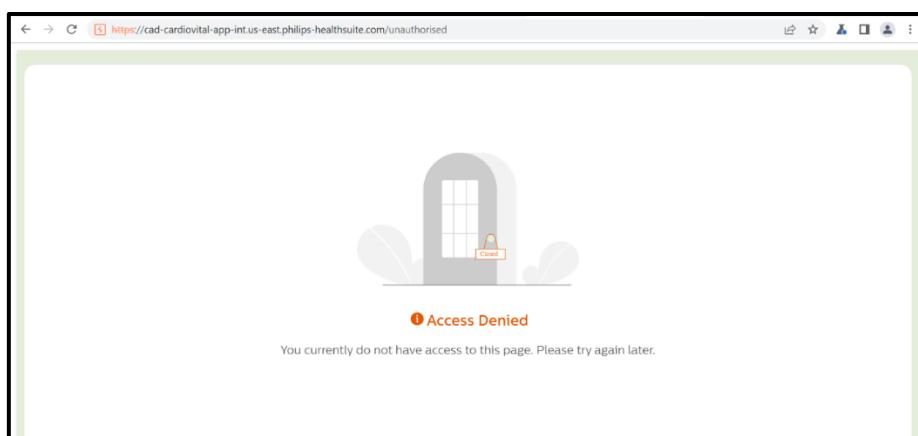
https://docs.philips.com/v/g/personal/chaitran_shivayogimath_philips_com/EU4LUJeoLGJGtqSQ0QJfjEBv8cjUEeWhVkJOG_ZFje5w?e=ULvMuz

Retest Status as of 10 Feb 2023:

It is observed that the Instance 1 is still reproduceable as seen in the screenshot below:



The Second instance is fixed as shown below:



PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



There is another instance:

https://cad-consumer-app-int.us-east.philips-healthsuite.com/?code=8545169a917ede5f8b84bf03b1ef3be556a2b6917c824c6346&login_hint=9916337921

POC:

A screenshot of a browser window titled "Guided Health Service". The address bar shows a URL with a long code. The developer tools are open at the bottom, with the "Elements" tab selected. A tooltip "Waiting for ca..." is visible. The network tab shows a request to "https://cad-consumer-app-int.us-east.philips-healthsuite.com/?code=e5840abefd090e75700eceaa11fbf74b91538bb058a3eea178f&login_hint=9845878". The status bar indicates "Dimensions: iPhone SE ▾ 375 x 667 77% No throttling".

A screenshot of a browser window titled "Guided Health Service". The address bar shows a URL with a long code. The main content area displays a circular icon with a hat and glasses, and the text "You've gone Incognito". Below it, a message says "Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved." A link "Learn more" is present. On the left, a section titled "Chrome won't save the following information:" lists "Your browsing history", "Cookies and site data", and "Information entered in forms". On the right, a section titled "Your activity might still be visible to:" lists "Websites you visit", "Your employer or school", and "Your internet service provider". At the bottom, a button "Block third-party cookies" is shown with a toggle switch set to "On".

PHILIPS SCOE

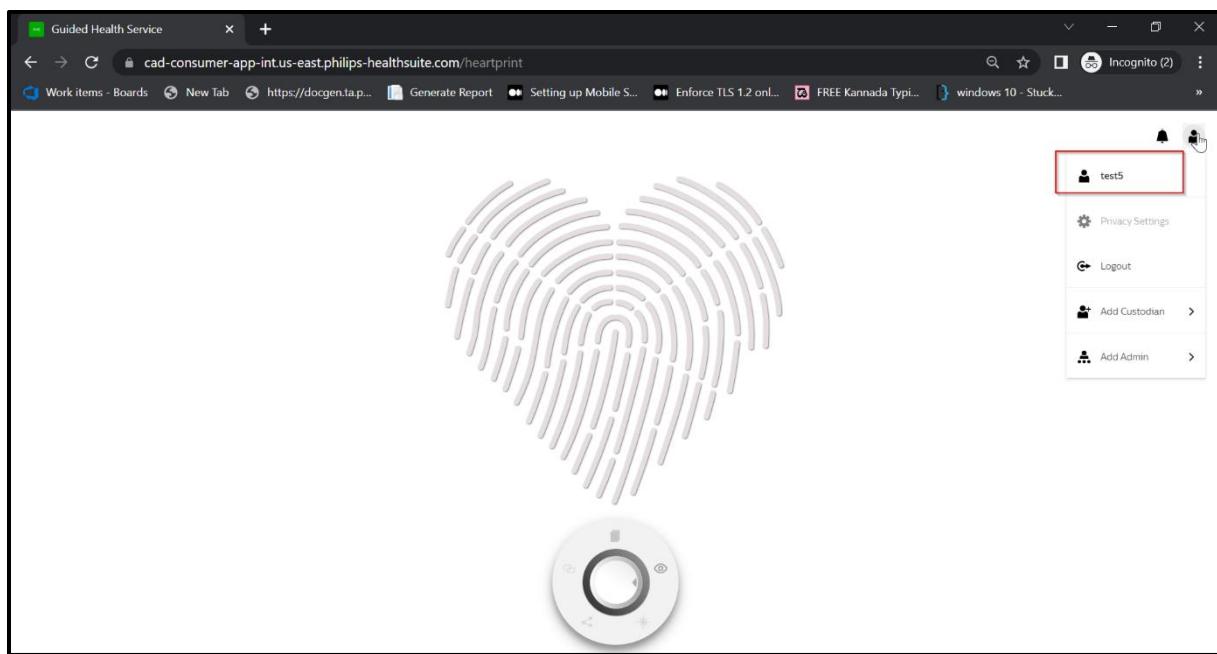
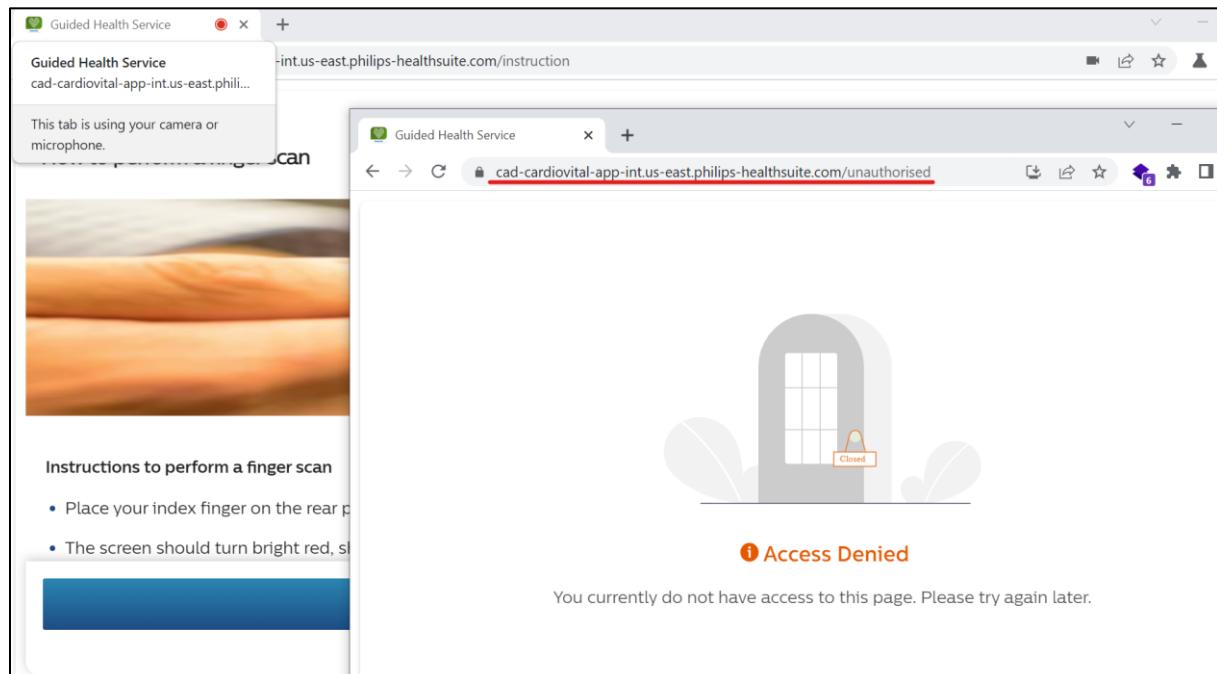


Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Resolution (17/April/2023):****Instance 1:**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Instance 3:**A screenshot of a Google Chrome browser window in Incognito mode. The address bar shows the URL: https://cad-consumer-app-int.us-east.philips-healtsuite.com/?code=1e58ed1041f7d4c475df1eacc77fea65fd1e6c125b1ce2f5d4&login_hint=9496980802. The main content area displays a circular icon with a hat and glasses, followed by the text "You've gone Incognito". Below this, it says "Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved." A link to "Learn more" is provided. To the right, there's a section titled "Chrome won't save the following information:" with a list of items, and another titled "Your activity might still be visible to:" with a list of items. At the bottom, there's a toggle switch for "Block third-party cookies" with the note "When on, sites can't use cookies that track you across the web. Features on some sites may break." The toggle switch is turned on.A screenshot of a web browser window titled "Guided Health Service". The address bar shows the URL: <https://cad-consumer-app-int.us-east.philips-healtsuite.com/signin>. The page itself has a blue header with the text "Your heartprint". Below the header is a Philips logo. The main content area features a "Login or Signup" button and the text "Great to have you. Let's get you started!". There is a text input field labeled "Enter mobile number" and a "login with email address" link. On the left side, there is a sidebar with sections for "Guidance" and "Vitals", which includes "Heart Rate: ... bpm" and "BP: .../... mmHg". A red box highlights the address bar of the browser window.

PHILIPS SCOE



Confidential

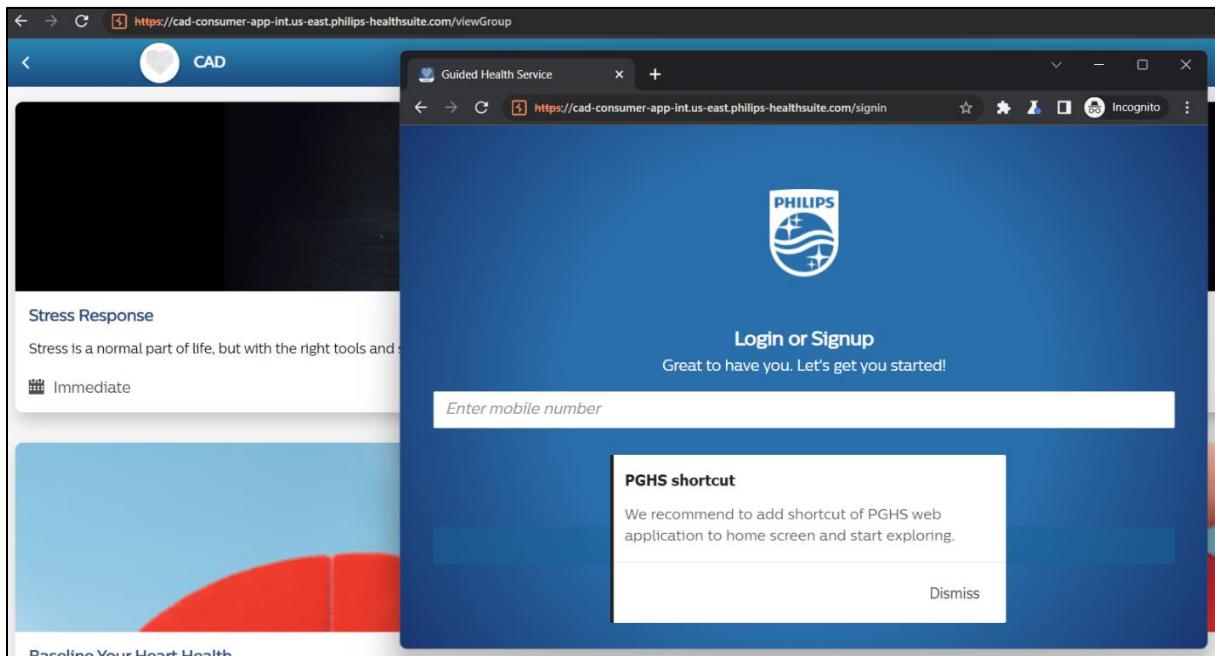
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Retest Status as of 24th July 2023



Authentication failed issue is fixed.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



7.3 Webapp: Modifiable Redirect URI Parameter

| | |
|------------------------|---|
| Vulnerability Title | Modifiable Redirect URI Parameter |
| Vulnerability Category | A5 Security Misconfiguration |
| Severity | Medium |
| CVSS V3 Calculation | CVSS Base Score: 5.3 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N |
| Description | <p>Vulnerability Description: During the assessment it was observed that for redirect_uri parameter which is user controllable. That parameter would help attacker to craft a request which would come to attacker hosted domain for user activation. Post which attacker can host that domain which resembles Philips original page, with this UI deception attacker can ask credentials from user and this way an adversary would be able to steal user credentials.</p> <p>Retest status(17/April/2023):</p> <p>It is observed that URL whitelisting for redirection is still absent. Hence the issue is OPEN.</p> <p>Retest status(26/April/2023):</p> <p>The issue still persists.</p> <p>Retest status (2/May/2023):</p> <p>URL whitelisting for redirection has been implemented properly. Hence marking this issue as 'CLOSED'.</p> <p>Retest as of 24-July-2023: The issue is fixed.</p> <p>Exploitability Rational: Since the URI parameter is accepted from client side and not validated on server side. This makes the attack relatively very easy. Attacker needs to craft request after which for user activation request would come to domain where attacker hosted a malicious page which looks like Philips website page. Having a similar character domain name victim can be fooled and hence make user believe on the fake URL. After this user enters credentials which would go to attacker and hence user account could be compromised.</p> |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



| | |
|---------------------------------|---|
| | Impact Rational: This would lead to user account compromise without much efforts from attacker. If user is using same password for other accounts & services then all such accounts could be impacted. |
| Affected Systems/IP Address/URL | https://cad-api-gateway-staging.us-east.philips-healthsuite.com/oauth/authorize?response_type=code,token,id_token&scope=openid&client_id=cad-client&redirect_uri=https://cad-consumer-app-staging.us-east.philips-healthsuite.com&login_hint=PHONE:9496980802&code_challenge=EUJnz05bd7FTk3IdKNO-gHi87o8RyYyRSz_K8oUKI4k&code_challenge_method=SHA256 |
| Recommendation | It is recommended to use URI parameter from whitelisted one, which is added by developer and not accepting it from user side. |
| Status | Closed |

Steps to Reproduce:

1. Configure browser to any proxy tool like burp.
2. Capture the oauth request with redirect_uri parameter.
3. Modify the parameter to any other Domain and it is observed that the redirect_uri can be modified and it redirects the user to the user supplied Domain.

Request

```

1 GET /oauth/authorize?response_type=code&scope=openid&client_id=cad-client&redirect_uri=https://evil.com?&login_hint=
HTTP/1.1 307 Temporary Redirect
2 Date: Mon, 12 Dec 2022 04:26:31 GMT
3 Expires: 0
4 Pragma: no-cache
5 Strict-Transport-Security: max-age=31536000 ; includeSubDomains
6 X-Content-Type-Options: nosniff
7 X-Frame-Options: DENY
8 X-Xss-Protection: 1 ; mode=block
9 X-Envoy-Upstream-Service-Time: 2043
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: close
15 Content-Length: 0
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
687
688
689
689
690
691
692
693
694
695
696
697
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1397
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1988
1989
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
204
```



Retest status as of 14 April, 2023:

The screenshot shows the Network tab of a browser developer tools interface. The request URL is `/oauth/authorize?response_type=code&token_id_token&scope=openid&client_id=cad-client&redirect_uri=https://evil.com`. The response is a `HTTP/1.1 307 Temporary Redirect` with a Location header pointing to `https://evil.com?code=cf81b0d83ff2851b314760ed2b12a6fe9e05562de616292f&login_hint=PHONE:9496980802&code_challenge=vzOjJ0oGzCnIyj7DmcxLkHgBIn-MqglnQw&code_challenge_method=SHA256`.

| Request | Response |
|--|---|
| <pre>1 GET /oauth/authorize?response_type=code&token_id_token&scope=openid&client_id=cad-client&redirect_uri=https://evil.com 2 Host: cad-api-gateway-int.us-east.philips-healthsuite.com 3 Cookie: SESSIONID=5082def7-bfd9-4e74-a1f8-6c0edb21130d 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36 7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 8 Sec-Fetch-Site: same-origin 9 Sec-Fetch-Mode: navigate 10 Sec-Fetch-User: ?1 11 Sec-Fetch-Dest: document 12 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="112" 13 Sec-Ch-Ua-Mobile: ?0 14 Sec-Ch-Ua-Platform: "Windows" 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 Connection: close 18</pre> | <pre>1 HTTP/1.1 307 Temporary Redirect 2 Cache-Control: no-cache, no-store, max-age=0, must-revalidate 3 Date: Fri, 14 Apr 2023 03:58:46 GMT 4 Expires: 0 5 Location: https://evil.com?code=cf81b0d83ff2851b314760ed2b12a6fe9e05562de616292f&login_hi nt=9496980802 6 Pragma: no-cache 7 Referrer-Policy: no-referrer 8 Server: envoy 9 Strict-Transport-Security: max-age=31536000 ; includeSubDomains 10 X-Content-Type-Options: nosniff 11 X-Envoy-Upstream-Service-Time: 80 12 X-Frame-Options: DENY 13 X-Vcap-Request-Id: ee58fd8d-e647-4baa-6162-397a9d011ec8 14 X-Xss-Protection: 1 ; mode=block 15 Content-Length: 0 16 Connection: Close 17 18</pre> |

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



The screenshot shows a NetworkMiner capture for the URL `https://evil.com`. The request is a GET for the root path, containing a code parameter and a login_hint. The response is an Apache 200 OK page with a Microsoft FrontPage 6.0 generated HTML content.

```
GET /?code=ae42972423df7568e9056bf168fa77f3da15113028b8190dca&login_hint=9496980802 HTTP/1.1
Host: evil.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Referer: https://cad-api-gateway-int.us-east.philips-healthsuite.com/

```

```
HTTP/1.1 200 OK
Date: Fri, 14 Apr 2023 04:00:00 GMT
Content-Type: text/html
Content-Length: 4166
Connection: close
Server: Apache/2
Last-Modified: Sat, 15 Jan 2022 23:21:33 GMT
ETag: "1046-5d5a7e2e24309e"
Accept-Ranges: bytes
Cache-Control: max-age=3600
Expires: Fri, 14 Apr 2023 05:00:00 GMT
Age: 0

```

```
<HTML>
<HEAD>
<meta content="Microsoft FrontPage 6.0" name="GENERATOR">
<meta content="FrontPage.Editor.Document" name="ProgId">
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<META NAME="GENERATOR" CONTENT="Microsoft FrontPage 6.0">
<title>
    Evil.Com - We get it...Daily.
</title>
<style>
    .serif{
        font-family:times,serif;
    }

```

January 15, 2022

Countup...

15

Sure, it's a new year, but we're in better shape right now than we were all of last year, except where we aren't.

Just remember that exhaustion doesn't mean it's done. It just means we're still working on it.

15 doesn't mean anything. Unless you think it does, then maybe it does. Just remember, it's always a good day to punch a Nazi, fascist, or fake patriot. The fake ones are the ones that scream the most about being patriots, while their actions show them to be Nazis or fascists.

[Read the Lies](#)

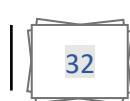
[Read the Shouts](#)

[Read the Truth](#)

PHILIPS SCOE

A horizontal line with diamond markers at both ends, indicating a scale or range.

Confidential



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Retest status as of 26 April, 2023:

Please refer the [Video POC](#)

Retest status as of 2 May, 2023:

Request

```

1 GET /oauth/authorize?response_type=code_token&scope=openid&client_id=
cad-client&redirect_uri=https://cad-api-gateway-staging.us-east.philips-healthsuite.com/login_hint=PHONE:94969808028
code_challenge=yTsd-qYGBclnIBwxdza6Hq1QYz7x95614g08ob15zv&code_challenge_method=
SHA256 HTTP/1.1
2 Host: cad-api-gateway-staging.us-east.philips-healthsuite.com
3 Cookie: SESSION=d01afea8-f793-475c-bd20-b10da6fb4fda
4 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="112"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/112.0.5615.138 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-site
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://cad-consumer-app-staging.us-east.philips-healthsuite.com/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19

```

Response

```

1 HTTP/1.1 307 Temporary Redirect
2 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
3 Date: Tue, 02 May 2023 06:20:00 GMT
4 Expires: 0
5 Location:
https://cad-consumer-app-staging.us-east.philips-healthsuite.com?login_hint=94969808028&error=1112
6 Pragma: no-cache
7 Referrer-Policy: no-referrer
8 Server: envoy
9 Strict-Transport-Security: max-age=31536000 ; includeSubDomains
10 X-Content-Type-Options: nosniff
11 X-Envoy-Upstream-Service-Time: 24
12 X-Frame-Options: DENY
13 X-Vcap-Request-Id: 87a94e7d-5b60-4e46-6a26-e699a4c42408
14 X-Xss-Protection: 1 ; mode=block
15 Content-Length: 0
16 Connection: Close
17
18

```

Request

```

1 GET /login_hint=94969808028&error=1112 HTTP/1.1
2 Host: cad-consumer-app-staging.us-east.philips-healthsuite.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/112.0.5615.138 Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Referer: https://cad-api-gateway-staging.us-east.philips-healthsuite.com/
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Connection: close
10
11

```

Response

```

1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, must-revalidate
3 Content-Type: text/html
4 Date: Tue, 02 May 2023 06:20:16 GMT
5 Etag: W/"644e95a6-9cc"
6 Last-Modified: Sun, 30 Apr 2023 16:21:58 GMT
7 Server: nginx
8 Vary: Accept-Encoding
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Vcap-Request-Id: 0d55f26d-80f9-4f3a-6c96-f53fe3e0d52
12 X-Xss-Protection: 1 ; mode=block
13 Content-Length: 2508
14 Connection: Close
15
16 <!doctype html><html lang="en">
<head>
    <meta charset="utf-8"/>
    <link rel="icon" href="./favicon.ico"/>
    <meta name="viewport" content="width=device-width, initial-scale=1,viewport-fit=cover"/>
    <meta name="description" content="Guided Health Services"/>
    <link rel="apple-touch-icon" sizes="180x180" href="./apple-touch-icon.png"/>
    <link rel="icon" type="image/png" sizes="32x32" href="./favicon-32x32.png"/>
    <link rel="icon" type="image/png" sizes="16x16" href="./favicon-16x16.png"/>

```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Retest Status as of 24th July 2023

Send Cancel < > Follow redirection Target: <https://cad-api-gateway-int.us-east.philips-healtsuite.com> HTTP/1

| Request | Response |
|---|---|
| <pre>Pretty Raw Hex 1 GET /oauth/authorize?response_type=code,token,id_token&scope=openid&client_id=cad-client 2 &redirect_uri=http://evil.com&login_hint=EMAIL:cadadmin@grr.la&code_challenge= 3 J7DRKSCRORKyeeRzHvhxtu5MF1qg9gJUmFjd-FUWUgcode_challenge_method=SHA256 HTTP/1.1 4 Host: cad-api-gateway-int.us-east.philips-healtsuite.com 5 Cookie: SESSION= 6 Sec-Ch-Ua: 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "" 9 Upgrade-Insecure-Requests: 1 10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36 11 Accept: 12 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 13 Sec-Fetch-Site: same-site 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-User: ?1 16 Sec-Fetch-Dest: document 17 Referer: https://cad-consumer-app-int.us-east.philips-healtsuite.com/ 18 Accept-Encoding: gzip, deflate 19 Accept-Language: en-US,en;q=0.9 20 Connection: close 21 22</pre> | <pre>Pretty Raw Hex Render 1 HTTP/1.1 302 Found 2 Cache-Control: no-cache, no-store, max-age=0, must-revalidate 3 Content-Security-Policy: default-src 'self' *.philips-healtsuite.com; 4 Date: Sun, 23 Jul 2023 06:26:24 GMT 5 Expires: 0 6 Location: 7 /oauth/login?response_type=code,token,id_token&scope=openid&client_id=cad-client&redirect_uri=http://evil.com&login_hint=EMAIL:cadadmin@grr.la&code_challenge=J7DRKSCRORKyeeRzHvhxtu5MF1qg9gJUmFjd-FUWUgcode_challenge_method=SHA256 8 Pragma: no-cache 9 Referrer-Policy: no-referrer 10 Server: envoy 11 Set-Cookie: SESSION=503c9e14-7daf-4d74-9496-0a31dc1e6df5; Path=/; 12 Domain=.us-east.philips-healtsuite.com; Max-Age=604800; Expires=Sun, 30 Jul 2023 13 06:26:25 GMT; Secure; HttpOnly; SameSite=Lax 14 Strict-Transport-Security: max-age=31536000 ; includeSubDomains 15 X-Content-Type-Options: nosniff 16 X-Envoy-Upstream-Service-Time: 16 17 X-Frame-Options: DENY 18 X-Vcap-Request-Id: a5f2d0d7-3fec-40b0-5a65-ab15cda65982 19 X-Xss-Protection: 1 ; mode=block 20 Content-Length: 0 21 Connection: Close 22</pre> |

Fixed Redirect issue

Send Cancel < > Follow redirection Target: <https://cad-consumer-app-int.us-east.philips-healtsuite.com> HTTP/1

| Request | Response |
|---|--|
| <pre>Pretty Raw Hex 1 GET /?login_hint=EMAIL:cadadmin@grr.la&error=1112 HTTP/1.1 2 Host: cad-consumer-app-int.us-east.philips-healtsuite.com 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36 5 Accept: 6 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 7 Referer: https://cad-api-gateway-int.us-east.philips-healtsuite.com/ 8 Accept-Encoding: gzip, deflate 9 Accept-Language: en-US,en;q=0.9 10 Connection: close 11 12</pre> | <pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Cache-Control: no-cache, must-revalidate 3 Content-Type: text/html 4 Date: Sun, 23 Jul 2023 06:27:04 GMT 5 Etag: W/"64b503eb-a8d" 6 Last-Modified: Mon, 17 Jul 2023 09:03:39 GMT 7 Server: nginx 8 Vary: Accept-Encoding 9 X-Content-Type-Options: nosniff 10 X-Frame-Options: SAMEORIGIN 11 X-Vcap-Request-Id: 7f1884f9-34ba-425d-4eaf-f1419c8eadfd 12 X-Xss-Protection: 1; mode=block 13 Connection: Close 14 Content-Length: 2701 15</pre> |

The issue is fixed

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



7.4 Webapp: Rate Limiting Not Implemented

| | |
|------------------------|--|
| Vulnerability Title | Rate Limiting Not Implemented |
| Vulnerability Category | A5 Security Misconfiguration |
| Severity | Medium |
| CVSS V3 Calculation | CVSS Base Score: 6.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H |
| Description | <p>Vulnerability Description: During security assessment it is observed that the application has not implemented Rate Limiting on Resend OTP request.</p> <p>Rate limiting is the process of controlling traffic rate from and to a server or component. It can be implemented on infrastructure as well as on an application level. Here the application does not implement rate limiting.</p> <p>Retest Status:</p> <p>It was observed that once the Request OTP request is sent for multiple times in a given time, the OTP will be received continuously after a long gap, we see a 200OK.</p> <p>When a legitimate user tries to login again, he will not be able to login as the server says Invalid OTP. As seen in the screenshots below. This causes a DOS to a legitimate user.</p> <p>Note: This is applicable to Custodian and Admin Login for email ids (Email Flooding).</p> <p>Retest Status(13/April/2023):</p> <p>It was observed that rate limit is still missing and causes DOS to a legitimate user when s/he tries to log in. Hence the issue is OPEN.</p> <p>Retest Status (05/May/2023):</p> <p>It was observed that rate limit is implemented in such a way that OTP enabling happens only for three times and then the functionality is blocked for 10 mins. This prevents DOS attack and hence marking this issue as 'CLOSED'.</p> <p>Retest as of 24-July-2023: The issue is fixed.</p> |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | |
|--|---|
| | <p>Exploitability Rational: An attacker who has access to the application URL and Valid user phone numbers/email ids.</p> <p>Impact Rational: As an impact, an attacker can send n number of requests to Resend OTP and availability of the server can be compromised and SMS/email can be flood to the end user.</p> |
| Affected Systems/IP Address/URL | https://cad-api-gateway-int.us-east.philips-healtsuite.com/oauth/otp |
| Recommendation | It is recommended to implement captcha to the login page which will help in evading the Bruteforce attacks and multiple requests being sent to the SMS Gateway. |
| Status | Closed |

Steps to Reproduce

1. Capture the Resend OTP request using any proxy tool like Burp.
2. Send the request to Intruder and repeat to send this request many times.
3. It is observed that the request can be sent many times.

The screenshot shows the Burp Suite interface with the following details:

- Attack** tab is selected.
- Results** tab is active.
- Filter: Showing all items** is applied.
- Request** tab is selected.
- Pretty** view is selected.
- Content-Type: text/plain; charset=UTF-8**
- Date: Thu, 15 Dec 2022 11:14:10 GMT**
- Expires: 0**
- Pragma: no-cache**
- Referrer-Policy: no-referrer**
- Server: envoy**
- Strict-Transport-Security: max-age=31536000 ; includeSubDomains**
- X-Content-Type-Options: nosniff**
- X-Envoy-Upstream-Service-Time: 32**
- X-Frame-Options: DENY**
- X-Vcap-Request-ID: 609307bf-c79-4db0-6280-8fb506a2b443**
- X-Xss-Protection: 1 ; mode-block**
- Content-Length: 7**
- Connection: close**
- SUCCESS**

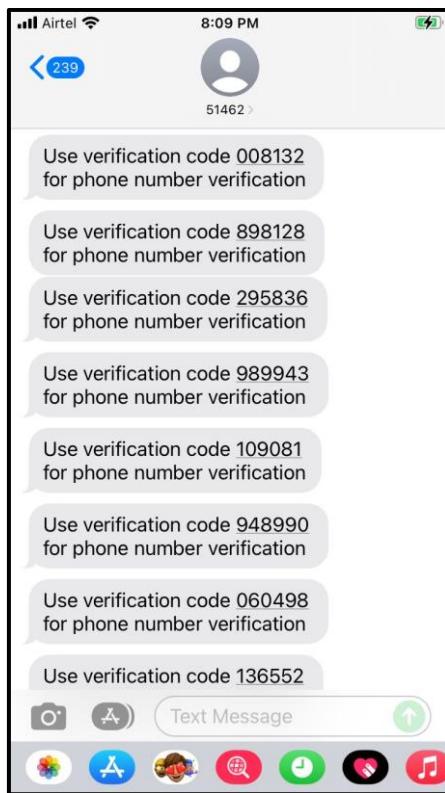
PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Retest Status as of 10 Feb 2023:**

It was observed that once the Request OTP request is sent for multiple times in a given time, the OTP will be received only 2 times but we see a 200 OK.

When a legitimate user tries to login again, he will not be able to login as the server says Invalid OTP. As seen in the screenshots below. This causes a DOS to a legitimate user.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Attack Save Columns
Results Positions Payloads Resource Pool Options

Filter: Showing all items

| Request | Payload | Status | Error | Timeout | Length | Comment |
|---------|------------|--------|-------------------------------------|-------------------------------------|--------|---------|
| 29 | 9738929763 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 960 | |
| 30 | 9738929763 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 961 | |
| 31 | 9738929763 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 960 | |
| 32 | 9738929763 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 960 | |
| 33 | 9738929763 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 960 | |
| 34 | 9738929763 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 960 | |
| 35 | 9738929763 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 960 | |
| 36 | 9738929763 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 960 | |
| 37 | 9738929763 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 960 | |
| 38 | 9738929763 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 960 | |
| 39 | 9738929763 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 960 | |
| 40 | 9738929763 | 200 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 960 | |

Request Response
Pretty Hex Render

```

6 Content-Type: text/plain; charset=UTF-8
7 Date: Fri, 03 Feb 2023 08:25:38 GMT
8 Expires: 0
9 Pragma: no-cache
10 Referrer-Policy: no-referrer
11 Server: envoy
12 Strict-Transport-Security: max-age=31536000 ; includeSubDomains
13 X-Content-Type-Options: nosniff
14 X-Envoy-Upstream-Service-Time: 70
15 X-Frame-Options: DENY
16 X-Vcap-Request-Id: 8c17ecb-3060-4d1e-77ae-cc107844939e
17 X-Xss-Protection: 1 ; mode-block
18 Content-Length: 7
19 Connection: close
20
21 SUCCESS

```

① ⌂ ⌂ ⌂ Search... 0 matches

Finished

← → ⌂ https://cad-api-gateway-int.us-east.philips-healthsuite.com/oauth/login?error

Confirm your verification code

Your verification code has been sent.

9738929763

Enter OTP

! Invalid OTP

Didn't receive the OTP? Request a new one in 38 seconds

Resend OTP

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Retest status as of 13 April,2023:

Screenshot of a security testing interface showing a list of requests and their corresponding responses.

Request List:

| Request | Payload | Status | Error | Timeout | Length | Comment |
|---------|----------|--------|--------------------------|--------------------------|--------|---------|
| 55 | 11111111 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 891 | |
| 56 | 1111 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 891 | |
| 57 | 485555 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 891 | |
| 58 | 11212121 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 891 | |
| 59 | 11111111 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 891 | |
| 60 | 1111 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 891 | |
| 61 | 485555 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 891 | |
| 62 | 11212121 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 891 | |
| 63 | 11111111 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 891 | |
| 64 | 1111 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 891 | |
| 65 | 454545 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 891 | |

Response Details:

```

1 HTTP/1.1 302 Found
2 Access-Control-Allow-Credentials: true
3 Access-Control-Allow-Origin: null
4 Access-Control-Expose-Headers:
    Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,Host,cache-control,content-type,content-transfer-encoding,Content-Type,Authorization,authorization,userid,edisp-introspect-value,Token,token,Access-Control-Allow-Origin,Origin,X-GHS-AUTH,api-version,*
5 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
6 Date: Tue, 11 Apr 2023 10:57:24 GMT
7 Expires: 0
8 Location: /auth/login?error
  
```

Bottom Navigation:

- Search bar: Search...
- Buttons: ? (Help), ⚙ (Settings), ⏪ (Back), ⏩ (Forward), ⏴ (List)
- Text: 0 matches

Finished

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

39

Printed copies are uncontrolled unless authenticated.



cad-api-gateway-int.us-east.philips-healthsuite.com/oauth/login?error

Confirm your verification code

Your verification code has been sent.

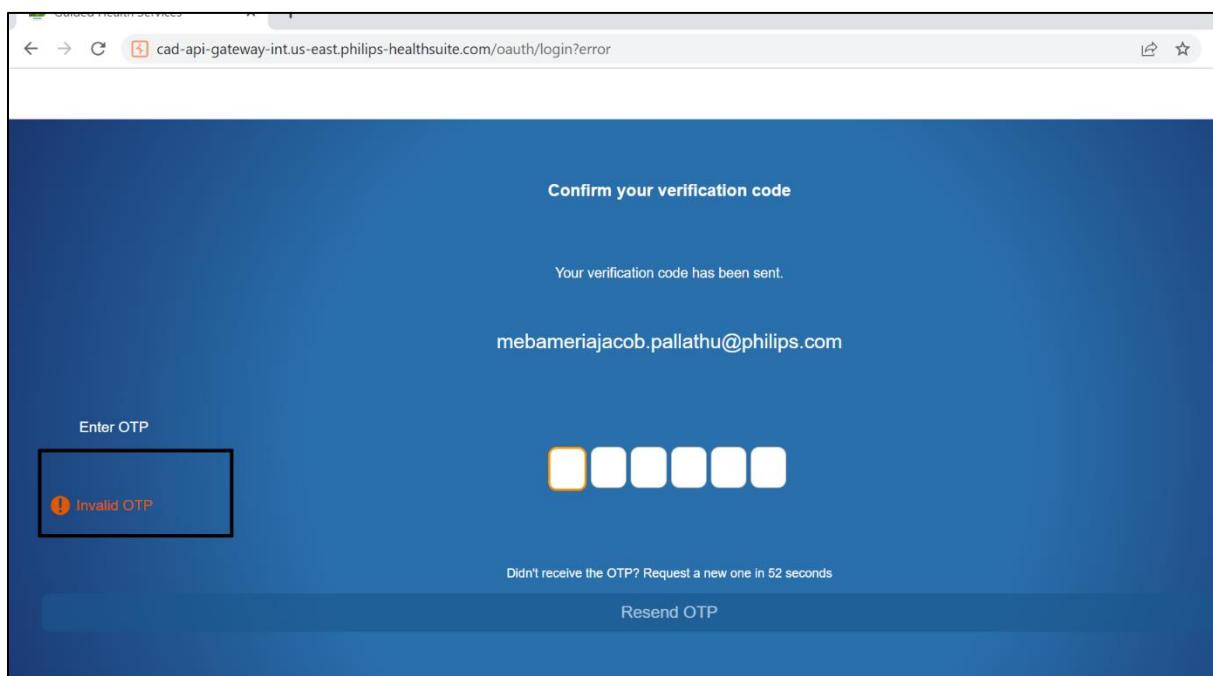
mebameriajacob.pallathu@philips.com

Enter OTP

Invalid OTP

Didnt receive the OTP? Request a new one in 52 seconds

Resend OTP



Retest status as of 05/May/2023:

Guided Health Services

cad-api-gateway-staging.us-east.philips-healthsuite.com/oauth/login

Confirm your verification code

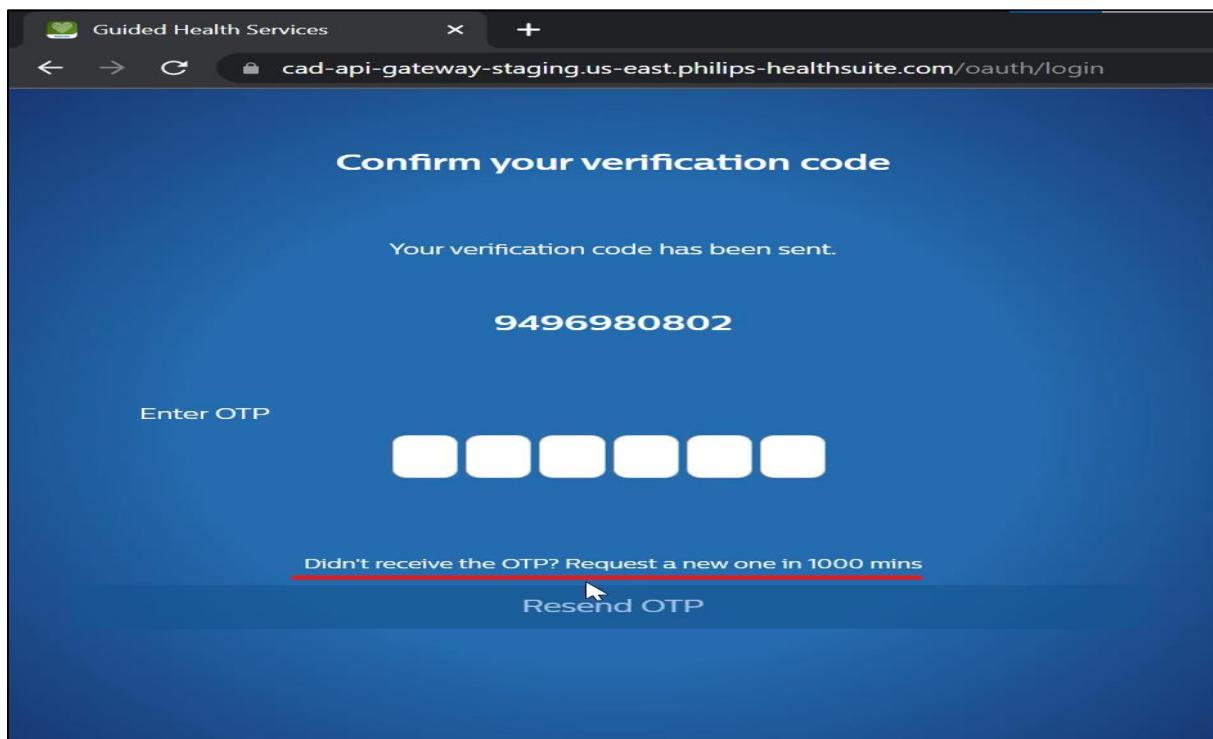
Your verification code has been sent.

9496980802

Enter OTP

Didnt receive the OTP? Request a new one in 1000 mins

Resend OTP



PHILIPS SCOE



Confidential

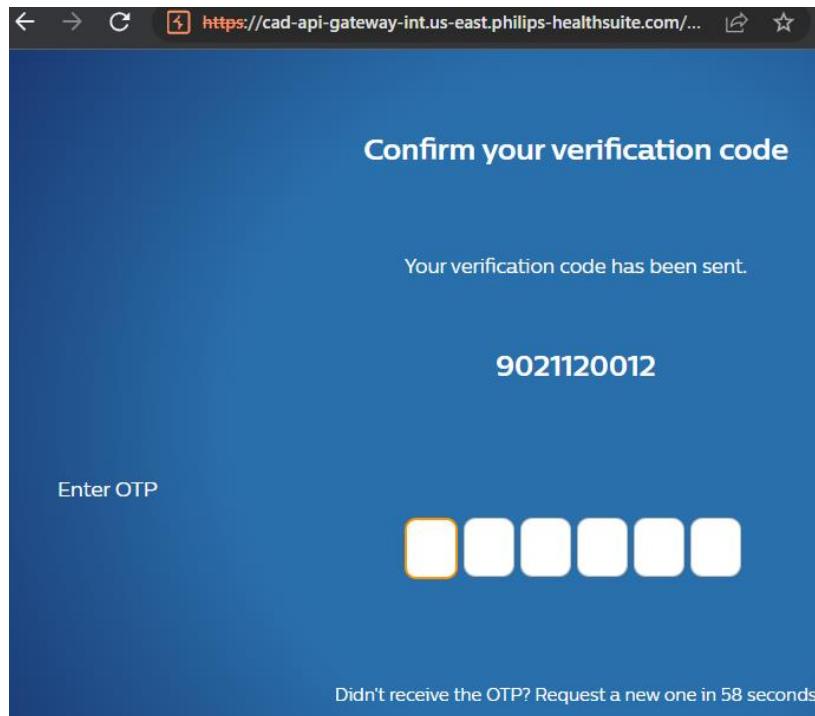
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Retest Status as of 24th July 2023



a. Screenshots shows that the attacker tried requesting for OTP to flood victim SMS-inbox

| 14. Intruder attack of https://cad-api-gateway-int.us-east.philips-heal... | | | | | | |
|--|-----------|-------------|--------------------------|--------------------------|--------|---------|
| Results | Positions | Payloads | Resource pool | Settings | | |
| Filter: Showing all items | | | | | | |
| Request | Payload | Status code | Error | Timeout | Length | Comment |
| 7 | abba | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1033 | |
| 6 | baba | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1032 | |
| 5 | aaba | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1031 | |
| 4 | bbaa | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1031 | |
| 3 | abaa | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1033 | |
| 2 | baaa | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1033 | |
| 1 | aaaa | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1033 | |

| Request | Response |
|---------|---|
| Pretty | Raw Hex Render |
| 1 | HTTP/1.1 200 OK |
| 2 | Access-Control-Allow-Credentials: true |
| 3 | Access-Control-Allow-Origin: https://cad-api-gateway-int.us-east.philips-heal... |
| 4 | Access-Control-Expose-Headers: |
| 5 | Accept, Accept-Encoding, Connection, Content-Length, keep-alive, user-agent, Host, cache-control, content-type, content-transfer-encoding, Content-Type, Authorization, authorization, user_id, edisp-introspect-via, Tid, Token, cookie, Access-Control-Allow-Origin, Origin, X-GHS-AUTH, api-version, * |
| 6 | Content-Expires: 0 |
| 7 | Content-Security-Policy: default-src 'self' *.philips-heal... |
| 8 | Content-Type: text/plain;charset=UTF-8 |
| 9 | Date: Mon, 24 Jul 2023 14:21:22 GMT |
| 10 | Expires: 0 |
| 11 | Pragma: no-cache |
| 12 | Referer-Policy: no-referrer |
| 13 | Server: envoy |
| 14 | Strict-Transport-Security: max-age=31536000 ; includeSubDomains |
| 15 | X-Content-Type-Options: nosniff |
| 16 | X-Envoy-Upstream-Service-Time: 44 |
| 17 | X-Frame-Options: DENY |
| 18 | X-Request-Id: 057c1e2a-7c8c-4a36-7f95-3692a180ea1c |
| 19 | X-Xss-Protection: 1 ; mode=block |
| 20 | Content-Length: 6 |
| 21 | Connection: Close |
| 22 | EXCEED |

b. Screenshots shows that the attacker used intruder to make OTP flood attack

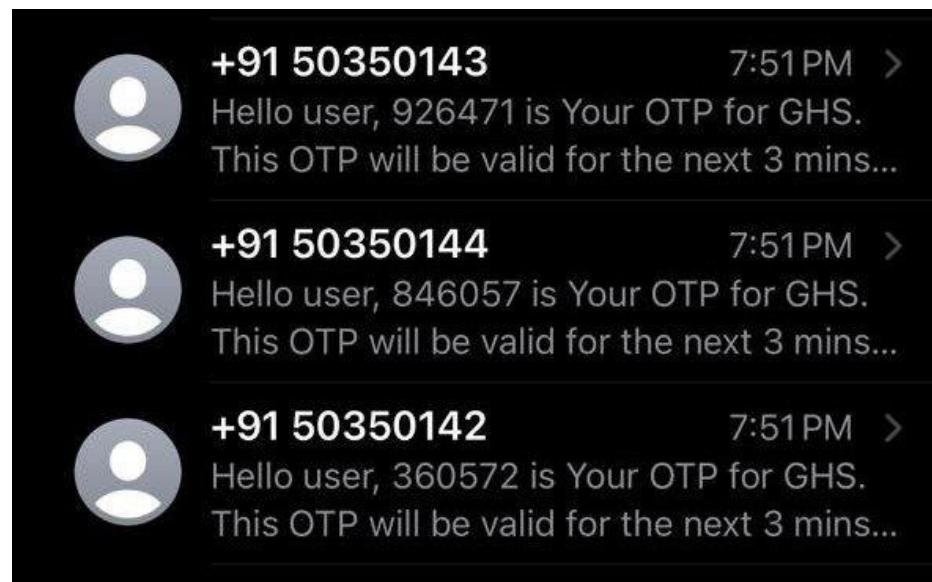
PHILIPS SCOE



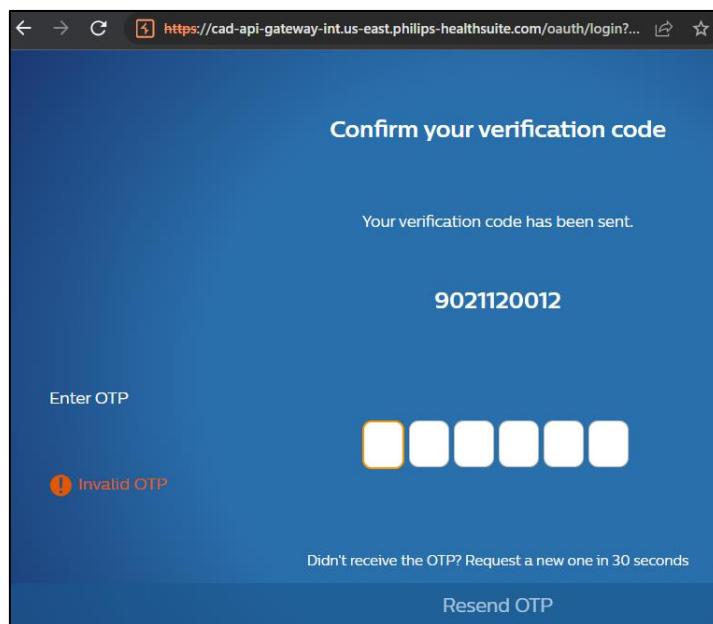
Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).





c. Screenshots shows that since rate limiting is enabled, victim will get only 3OTPs



d. Screenshots shows that the Old OTP cannot be reused within 4minutes



7.5 Webapp: Client Side Validation Bypass

| | |
|------------------------|---|
| Vulnerability Title | Client Side Validation Bypass |
| Vulnerability Category | A5 Security Misconfiguration |
| Severity | Informational |
| CVSS V3 Calculation | CVSS Base Score: NA CVSS Vector: NA |
| Description | <p>Vulnerability Description: During the security assessment of the product, it was observed that the Resend OTP button will be disabled for 60s, but it can be bypassed by removing the disabled button and can be enabled any number of times from the application frontend.</p> <p>Retest status(17/April/2023):</p> <p>Resend OTP button can be enabled by bypassing the client-side validation. Hence the issue is OPEN.</p> <p>Retest status (26/April/2023):</p> <p>The issue still persist.</p> <p>Retest status(05/May/2023):</p> <p>It was observed that Resend OTP button can be enabled by bypassing the client side validation but OTP will be sent only for three times and after that, the functionality will be blocked for 10 mins. Hence the severity of this issue is reduced to Observational/Informational. Though we can enable the button, the OTP is triggered only thrice and for next ten mins OTP is blocked.</p> <p>Retest as of 24-July-2023: The issue is fixed.</p> <p>Exploitability Rational: Any user who has access to Application can exploit this issue.</p> <p>Impact Rational: An attacker can send as many Resend OTP requests for any user and availability can be compromised.</p> |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | |
|---------------------------------|--|
| Affected Systems/IP Address/URL | https://cad-api-gateway-staging.us-east.philips-healthsuite.com/oauth/login |
| Recommendation | In either cases, it has to be made sure that the Resend OTP button is not enabled unless the desired action is fulfilled. Furthermore, the server should validate if the client side actions fulfill the requirement or not. |
| Status | Closed |

Steps to Reproduce

Refer the video POC in the below location:

https://docs.philips.com/:v:/g/personal/chaitran_shivayogimath_philips_com/Ed-XAA2AQPpAusv8mTPCZEkBdIX6cp4H88kw9P0ZVPylQw?e=frjRIG

Retest status as of 17/April/2023:

https://docs.philips.com/:v:/g/personal/mebameriajacob_pallathu_philips_com/EX4dzX35Md5Cmic9_zF1L4QB3HNYy4h5ZuNoain3QUrIw?e=dWuGDJ

Retest status as of 26/April/2023:

https://docs.philips.com/:v:/g/personal/mebameriajacob_pallathu_philips_com/ET37o19XT7ICmM_Ght8uDiABEaEjLhjeQJE5Y4upLRvzoA?e=FuOegw

Retest status as of 05/May/2023:

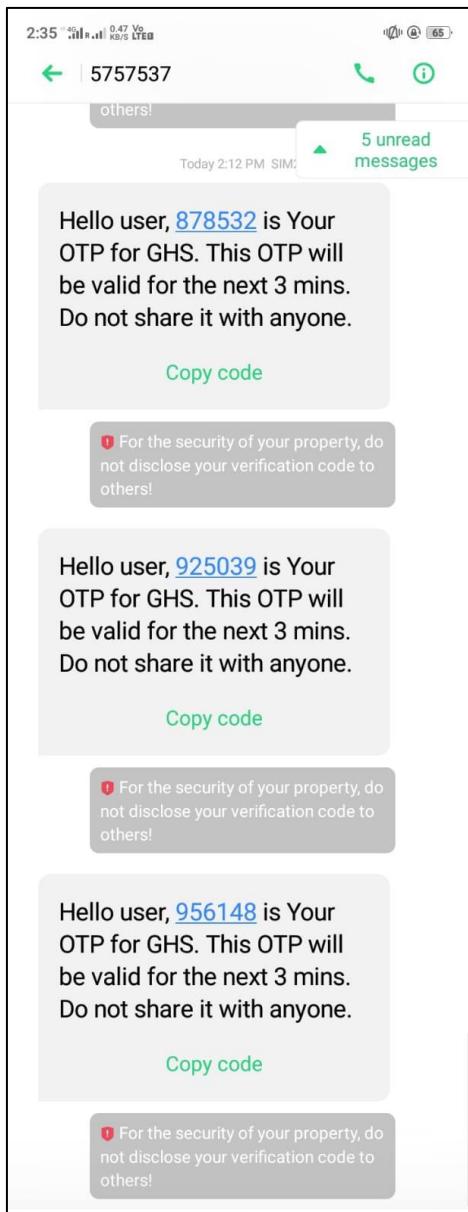
https://docs.philips.com/:v:/g/personal/mebameriajacob_pallathu_philips_com/EYIs6jHdIBBDlr3vZDFAIQBRAKc71TD1HGxjarAbssLwQ?e=qw65aV

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Retest Status as of 24th July 2023**A screenshot of a web browser displaying a verification code page. The title is "Confirm your verification code". Below it, a message says "Your verification code has been sent." A large 6-digit OTP "9021120012" is displayed. Below the OTP is a text input field labeled "Enter OTP" and a row of six empty input boxes for entering the code. At the bottom is a "Resend OTP" button.

Confirm your verification code

Your verification code has been sent.

9021120012

Enter OTP

Resend OTP

a. Click on Resend OTPA screenshot of the same verification code page after a user has clicked the "Resend OTP" button. An orange error message "Invalid OTP" appears below the input fields. The "Resend OTP" button is now grayed out and disabled. The developer tools' Elements tab is open, showing the HTML structure of the resend button with the id "OTPButton" and its disabled state.

Confirm your verification code

Your verification code has been sent.

9021120012

Enter OTP

Invalid OTP

Didn't receive the OTP? Request a new one in 47 seconds

Resend OTP

Elements Console Sources Network Performance Memory Application >

```
<div id="CountdownTimerDiv" class="verify-code-request-otp-text" data-langkey="verifycode.requestnew.otp">--</div>
<button id="OTPButton" type="button" onclick="handleResendButtonClick()" disabled data-langkey="verifycode.resend.otp">Resend OTP </button> -- $0
```

b. Once we clicked, Resend OTP will be disabled

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



The screenshot shows a 'Confirm your verification code' page. At the top, it says 'Your verification code has been sent.' Below that is the verification code '9021120012'. There is an input field labeled 'Enter OTP' with six empty boxes for digits. An error message 'Invalid OTP' is displayed below the input field. Below the input field is a link 'Didn't receive the OTP? Request a new one in 22 seconds' and a 'Resend OTP' button. The browser's developer tools are open, specifically the 'Elements' tab, which shows the HTML structure of the 'Resend OTP' button.

- c. Try Enabling the Resend OTP option by inspect element, remove Disabled option, and again click on Resend OTP

The screenshot shows the same 'Confirm your verification code' page as the previous one. The 'Resend OTP' button is now enabled (not grayed out). An error message 'You have reached OTP Re-send limit. Retry after some time.' is displayed below the input field.

- d. After Resend OTP, Application shows error message like Reached OTP Re-send Limit. From Server end OTP will not be sent to the user.



7.6 Webapp: Weak SSL/TLS configuration

| | |
|------------------------|--|
| Vulnerability Title | Weak SSL/TLS configuration |
| Vulnerability Category | A2 Cryptographic Failures |
| Severity | Medium |
| CVSS V3 Calculation | CVSS Base Score: 7.1 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L |
| Description | <p>Vulnerability Description:</p> <p>Case 1,2: During the security assessment, it was observed that the application supports communication using TLS 1.0 and TLS 1.1.</p> <p>TLS 1.0 has a number of cryptographic design flaws. The server-side SSL/TLS endpoint is configured to allow connections using TLS protocol version 1.0 ("TLSv1.0"), which contains known weaknesses. The TLS protocol provides secure transport between endpoints over a network, with the intended effect of offering data integrity and confidentiality. Certain configurations of TLS version 1.0 are vulnerable to known man-in-the-middle ("MitM") attacks, including the BEAST and POODLE attacks. In addition, multiple standards organizations including NIST and PCI have declared that TLSv1.0 no longer provides sufficient data protection.</p> <p>Note: This issue is a High severity issue as per SCoE. Since this is affected by the AWS S3 buckets, which is a known issue and Philips does not have control over the S3 buckets to disable the TLSv1.0 and 1.1 support we are reporting it as a Medium Severity issue. The Product team should approach Amazon to disable the TLSv1.0 and 1.1 support.</p> <p>Case 3: One of the TLS/SSL certificates used by your server is about to expire(Wed Sep 06 2023). Once the certificate has expired, most web browsers will present end-users with a security warning, asking them to manually confirm the authenticity of your certificate chain. Software or automated systems may silently refuse to connect to the server.</p> <p>Reference: https://media.defense.gov/2021/Jan/05/2002560140/-1-1/0/ELIMINATING_OBSOLETE_TLS_U00197443-20.PDF</p> |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | |
|--|---|
| | <p>Retest(17/April/2023):</p> <p>AWS S3 buckets are still in use and therefore TLS 1.0 and TLS 1.1 are being used for the communication. Hence the issue is OPEN.</p> <p>Case 1,2: Retest as of 24-July-2023: The issue still exist.</p> <p>Case 3: Test as of on 24 July 2023: Server certificate is about to expire. Issue is open.</p> <p>Exploitability Rational: Weaknesses in TLSv1.0, v1.1 connections may allow an attacker to decrypt traffic passed between a victim's client and the server.</p> <p>Case 3: Exploitability can be performed by accessing the webapplication, once the SSL certificate is expired, attacker can perform MITM attacks and capture every request which is send by victim.</p> <p>Impact Rational: Any sensitive information passed over this connection may be exposed.</p> <p>Case 3: If an application server detects an expired certificate with a system it is communicating with, the application server may continue processing data as if nothing happened, or the connection may be abruptly terminated.</p> |
| Affected Systems/IP Address/URL | https://cf-s3-26970c8a-1c38-425f-8f35-eaf0dc44f734.s3.amazonaws.com https://cad-api-gateway-int.us-east.philips-healtsuite.com/ https://cad-consumer-app-int.us-east.philips-healtsuite.com/ |
| Recommendation | <p>Case 1,2: It is advised to support TLS1.2 and TLS1.3 and disabling older protocols (not supporting for backward compatibility).</p> <p>Case 3: Contact your Certificate Authority to renew the SSL certificate.</p> |
| Status | Open |

Steps to Reproduce

- Run the sslscan scan by executing the Nmap NSE Scan:

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).





2. nmap -Pn -sS -p 443 --script ssl* <hostname>

Retest Evidence as of 18 Apr 2023:

```
nmap -sS -p 443 -Pn --script ssl* cf-s3-26970c8a-1c38-425f-8f35-eaf0dc44f734.s3.amazonaws.com
Nmap 7.7.1 (https://nmap.org) starting at 2023-04-18 10:44:10 UTC
...
ssl-enum-ciphers:
  TLSv1.0:
    ciphers:
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
      TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
      TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
      TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
      TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
      TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
      TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
      TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
  compressors:
    NULL
  cipher preference: server
  warnings:
    64-bit block cipher 3DES vulnerable to SWEET32 attack
  TLSv1.1:
    ciphers:
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
      TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
      TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
      TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
```

Refer [section 9](#) for detailed nmap ssl scan results.

Retest Status as of 24th July 2023

Case 1: <https://cad-consumer-app-int.us-east.philips-healthsuite.com/>

```
Nmap scan report for cad-consumer-app-int.us-east.philips-healthsuite.com (54.161.119.237)
Host is up (0.0099s latency).
Other addresses for cad-consumer-app-int.us-east.philips-healthsuite.com (not scanned): 52.87.118.180
rDNS record for 54.161.119.237: ec2-54-161-119-237.compute-1.amazonaws.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE     SERVICE
80/tcp    open      http
443/tcp   open      https
|_ ssl-enum-ciphers:
  TLSv1.2:
    ciphers:
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
      TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
      TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
      TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
      TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
    compressors:
      NULL
    cipher preference: server
  least strength: A
```

Identified Weak TLS CBC Cipher with NMAP Scan

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| Protocols | |
|-----------|-----|
| TLS 1.3 | No |
| TLS 1.2 | Yes |
| TLS 1.1 | No |
| TLS 1.0 | No |
| SSL 3 | No |
| SSL 2 | No |

| Cipher Suites | |
|--|--|
| # TLS 1.2 (suites in server-preferred order) | [button] |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) | ECDH secp256r1 (eq. 3072 bits RSA) FS 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) | ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 128 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) | ECDH secp256r1 (eq. 3072 bits RSA) FS 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) | ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 256 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) | WEAK 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) | WEAK 128 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) | WEAK 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) | WEAK 256 |

Identified Weak TLS CBC Cipher under SSL Labs Scan

Case 2: <https://cf-s3-26970c8a-1c38-425f-8f35-eaf0dc44f734.s3.amazonaws.com>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Nmap Output Ports / Hosts Topology Host Details Scans

```
nmap -sS -p 443 -Pn --script ssl* cf-s3-26970c8a-1c38-425f-8f35-eaf0dc44f734.s3.amazonaws.com
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
```

Hosts Services

OS ▾ Host

cf-s3-26970c8a-1c38-425f-8f35-eaf0dc44f734.s3.amazonaws.com

Filter Hosts

Identified Weak TLS CBC Cipher with NMAP Scan

| Configuration | |
|----------------|-----------|
| | Protocols |
| TLS 1.3 | No |
| TLS 1.2 | Yes |
| TLS 1.1 | Yes |
| TLS 1.0 | Yes |
| SSL 3 | No |
| SSL 2 | No |

Identified Weak TLS CBC Cipher under SSL Labs Scan

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Cipher Suites

TLS 1.2 (suites in server-preferred order)

| | | | |
|--|------------------------------------|----|------|
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) | ECDH secp256r1 (eq. 3072 bits RSA) | FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) | ECDH secp256r1 (eq. 3072 bits RSA) | FS | 256 |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc88) | ECDH secp256r1 (eq. 3072 bits RSA) | FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) | ECDH secp256r1 (eq. 3072 bits RSA) | FS | WEAK |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) | ECDH secp256r1 (eq. 3072 bits RSA) | FS | WEAK |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | ECDH secp256r1 (eq. 3072 bits RSA) | FS | WEAK |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) | ECDH secp256r1 (eq. 3072 bits RSA) | FS | WEAK |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) | WEAK | | 128 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) | WEAK | | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) | WEAK | | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) | WEAK | | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | WEAK | | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) | WEAK | | 256 |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) | WEAK | | 112 |

Identified Weak TLS CBC Cipher under SSL Labs Scan

TLS 1.1 (suites in server-preferred order)

| | | | | |
|--|------------------------------------|----|------|-----|
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) | ECDH secp256r1 (eq. 3072 bits RSA) | FS | WEAK | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | ECDH secp256r1 (eq. 3072 bits RSA) | FS | WEAK | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) | WEAK | | | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | WEAK | | | 256 |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) | WEAK | | | 112 |
| <hr/> | | | | |
| # TLS 1.0 (suites in server-preferred order) | | | | |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) | ECDH secp256r1 (eq. 3072 bits RSA) | FS | WEAK | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | ECDH secp256r1 (eq. 3072 bits RSA) | FS | WEAK | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) | WEAK | | | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | WEAK | | | 256 |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) | WEAK | | | 112 |

Identified Weak TLS CBC Cipher under SSL Labs Scan

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Case 3:****Test Evidence as of on 24 July 2023:**

```
SSL Certificate:  
Signature Algorithm: sha256WithRSAEncryption  
RSA Key Strength: 2048  
  
Subject: *.us-east.philips-healthsuite.com  
Altnames: DNS:*.us-east.philips-healthsuite.com, DNS:us-east.philips-healthsuite.com  
Issuer: DigiCert TLS RSA SHA256 2020 CA1  
  
Not valid before: Aug 10 00:00:00 2022 GMT  
Not valid after: Sep 5 23:59:59 2023 GMT
```

Server certificate is about to expire

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



7.7 Webapp/WebServices: Improper Session Management

| | |
|------------------------|---|
| Vulnerability Title | Improper Session Management |
| Vulnerability Category | A7 Identification and Authentication Failures |
| Severity | Medium |
| CVSS V3 Calculation | CVSS Base Score: 6.1 CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N |
| Description | <p>Vulnerability Description:</p> <p>Case 1: It was observed that session id is not invalidated at the server side due to which session id of one user can be used for the other user.</p> <p>Case 2: The application allows concurrent sessions: It was observed that upon deletion of user account, if the user is already logged in to the application via different browser, the existing session remain alive without any restrictions. Once the user logs out, then that user needs to sign up again to access the application. But until then that user can access and perform all operations.</p> <p>Case 3: If there are multiple tabs opened in same browser window and if the user initiates log out in one tab, then it is observed that the other parallel tabs are not automatically brought to login page. (Ideally immediately all tabs for same hostname should be redirected to login page post logout)</p> <p>Case 4: It was observed that the application does not log the user out after a reasonable period of inactivity. Inactivity timeout periods vary depending on the sensitivity of the data and functionality the application contains, but idle sessions longer than 15-30 minutes are typically considered vulnerable.</p> <p>Case 5: It was observed that if a user has logged into the application and closed the browser without logging out, then if the application is accessed, it is not brought to log in page. The tokens get regenerated and one can perform actions even without the need of log in.</p> |



| | |
|--|--|
| | <p>Retest as of 24-July-2023: The issue is still valid and not fixed.</p> <p>Exploitability rational</p> <p>For the case 1, attacker should have access to the application. For the case 2, user needs to be logged in to the application. For the case 3, user need to be logged in to the application in two or more different tabs of same browser window. For the case 4 and case 5 to be exploited, the attacker needs physical access to the system.</p> <p>Impact Rational: Leaving the user's session active after the user initiates logout provides the attacker with a larger window in which to steal a victim's session and impersonate that user in the application. The session token can be obtained through various techniques, such as intercepting network traffic ("Man-in-the-Middle" or "MitM"), Cross-Site Scripting (XSS), Cross-Site Tracing (XST), and in the case of URL-based session token transmission, local inspection of browser history. In addition to prolonging the session identifier's exposure to attack, failing to invalidate the user's session server-side also leaves the user with no way to deny an attacker's access once the victim discovers that their session has been compromised.</p> |
| Affected Systems/IP Address/URL | <p>https://cad-consumer-app-int.us-east.philips-healthsuite.com/home</p> <p>https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report</p> |
| Recommendation | <p>The user's HTTP session should be terminated on the server immediately after a logout action is performed. It is important to note that simply deleting the cookie from the browser will not terminate the server session. The session must be invalidated at the server, using the HTTP container's intrinsic session abandonment mechanism.</p> <p>Reference: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html</p> |
| Status | Open |



Steps to Reproduce:

Case 1:

Step 1: In 1 browser log in to the application as user A.

Step 2: In 2nd browser, log in as user B.

Step 3: Capture the scan request from 2nd browser.

Step 4: Replace the session id of 'A' with that of 'B'.

Refer the [Video POC](#) for more information.

Case 2:

Step 1: Log in to the application in two different browsers.

Step 2: Delete the user account from 1 browser.

Step 3: Observe that the session remains active in the other browser and the user can perform all actions.

Refer the [Video POC](#) for more information.

Case 3:

Step 1: Log into the application

Step 2: In the same browser window, log into the application in a different tab.

Step 3: Log out from the application in one tab, observe the adjacent tabs are not brought to the login page. Refer the below screenshot:

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



The screenshot shows a web browser window with two tabs open. Both tabs have the URL <https://cad-consumer-app-int.us-east.philips-healthsuite.com/cues>. The left tab displays a login screen with fields for 'Email or Sign in ID' and 'Password'. The right tab shows a green header bar and a main content area asking if the user has ever been told they have a heart problem. Below this, there are two radio button options: 'Yes' and 'No'.

Case 5:

Refer the [Video POC](#) for more information

Retest Status as of 24th July 2023:

Case 1:

The screenshot shows a web browser with a list of user profiles on the left. A 'Cookie Editor' dialog box is overlaid on the page, specifically showing a 'SESSION' cookie with the name 'SESSION' and value '91409590-114b-4f91-ae9f-08275b83975c'. There are buttons for '+' and '-' at the bottom of the dialog.

a. Screenshot shows that the Admin session is active in Browser A

PHILIPS SCOE

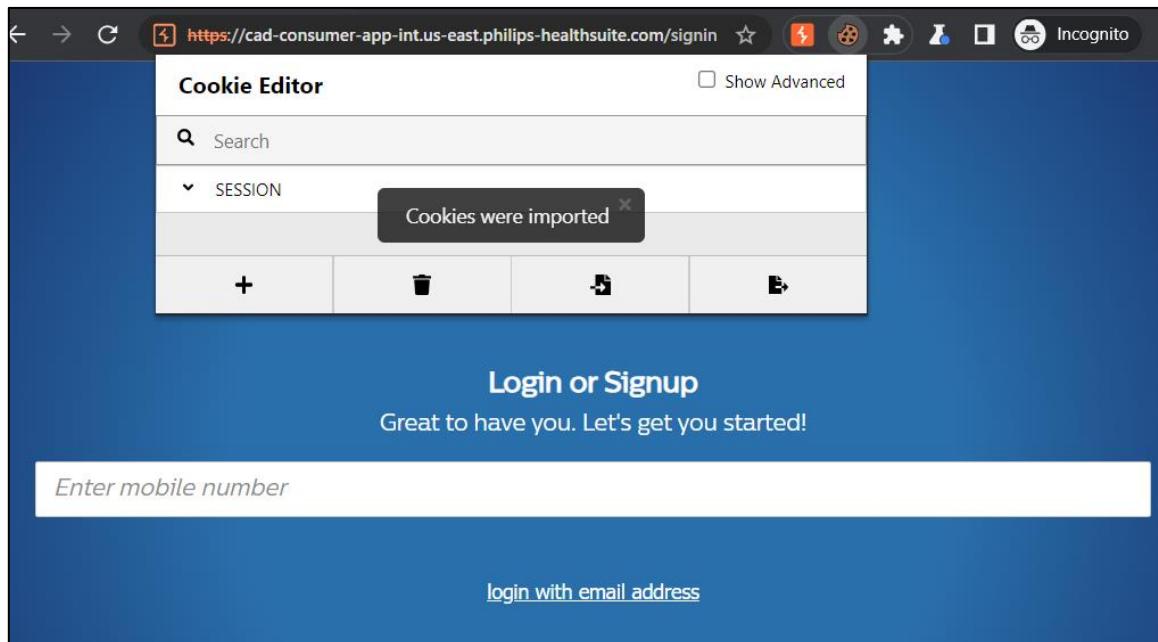


Confidential

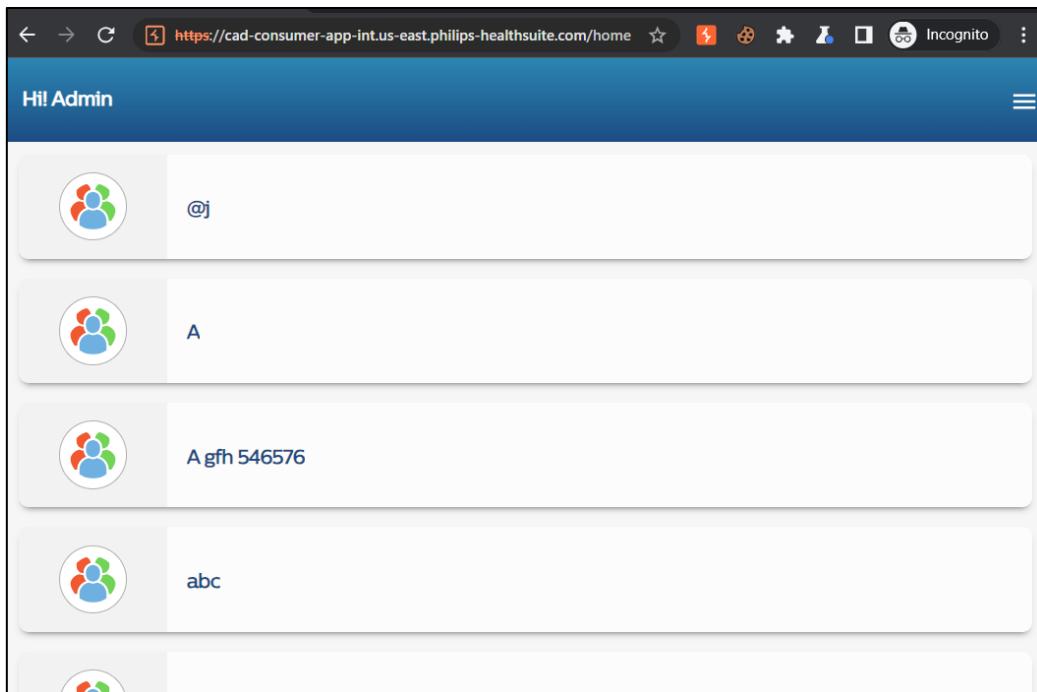
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



b. Screenshots shows that the Admin session cookie is imported to Browser B with signin page



c. Screenshot shows that once we refresh the Browser B, we will be login as Admin

Refer the [Video POC](#)

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Case 2:**Refer the [Video POC](#)**Case 3:**Refer the [Video POC](#)**Case 4:**

The screenshot shows a Microsoft Edge browser window with developer tools open. The main content area displays a mobile application interface for 'Beats Journey' titled 'Baseline Your Heart Health'. The developer tools panel on the right shows several errors in the 'Console' tab, primarily related to JSON parsing issues and missing attributes. The Windows taskbar at the bottom includes icons for File Explorer, Task View, and other system applications.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



The screenshot shows a web browser window with the URL cad-consumer-app-int-us-east.philips-healtsuite.com/home. The main content area displays a user profile for 'Hil Tom' and a 'Beats Journey' titled 'Baseline Your Heart Health'. The journey has 10 steps, with one completed. A message says 'Great work! See you tomorrow'. Below the journey are 'View Result' and 'Start' buttons. The developer tools sidebar on the right shows 1 issue: 'opened service-worker.js:1 cache'. It includes an error message: 'DevTools failed to load source map: Could not load content for https://cad-consumer-app-int-us-east.philips-healtsuite.com/service-worker.js.map. Unexpected token <'. The bottom status bar shows the date and time: 28-07-2023 18:22.

Session time out should be shorter period of time. Session was still logged in after 60minutes.

Case 5:

Refer the [Video POC](#)

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



7.8 Webapp: Lack of Authorization

| | |
|---------------------------------|---|
| Vulnerability Title | Lack of Authorization |
| Vulnerability Category | A1 Broken Access Control |
| Severity | Medium |
| CVSS V3 Calculation | CVSS Base Score: 6.8 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N |
| Description | <p>Vulnerability Description: The application lacks sufficient controls to prevent a user from accessing another user's functionality. It was observed that a non-admin user can see and modify an admin user's functionality because of lack of authorization check at server side.</p> <p>Retest status (27/April/2023):</p> <p>Authorization is still not implemented properly. Hence the issue is OPEN.</p> <p>Retest status(2/May/2023):</p> <p>Proper authorization check is in place and thereby marking this issue as 'CLOSED'.</p> <p>Retest as of 24-July-2023: The issue is Fixed.</p> <p>Exploitability Rational: The attacker needs to be an authenticated user.</p> <p>Impact Rational: Confidentiality and integrity are compromised and functionalities can be misused.</p> |
| Affected Systems/IP Address/URL | https://cad-api-gateway-staging.us-east.philips-healthsuite.com/identity/Search |
| Recommendation | Proper authorization mechanism should be implemented on server side, validating user's access to certain resources. Explicitly check the authorization on the server-side to verify that the user making a request to view data or perform an action is authorized to do. This is simple as checking that a user is authorized to view a particular page in the application or check that the user is authorized to |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | |
|--------|---|
| | perform an action overall. Many other more fine-grained situations may exist depending on the application context and the complexity of the business functionality. Reference: https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html |
| Status | Closed |

Supportive Evidence:

Refer the [Video POC](#) (non-admin user can see the resources of an admin user)

Refer the [Video POC](#) (non-admin user can see the custodian requests and after modifying the profile type from custodian to admin, able to see admin requests)

Retest status as of 27 April 2023:

Refer the [Video POC](#) (first instance is fixed)

Refer the [Video POC](#) (non-admin users can still see the custodian requests and admin requests)

Retest status as of 2 May 2023:

Refer the [Video POC](#)

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Retest Status as of 24th July 2023

Request

| | | | | |
|--------|-----|-----|----------------|-----------------|
| Pretty | Raw | Hex | JSON Web Token | JSON Web Tokens |
|--------|-----|-----|----------------|-----------------|

```

1 POST /identity/Search HTTP/1.1
2 Host: cad-api-gateway-int.us-east.philips-healhtsuite.com
3 Cookie: SESSION=91409590-114b-4f91-ae9f-08275b83975c
4 Content-Length: 43
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Mobile: ?0
7 Authorization: Bearer eyJhbGciOiJSUzIiNiIsImp0aSI6Ik1uWtVNREV3TVRvd01EUTB0enBoTmptaU9XWmxZbvJsiLwihLwjoiSlduIn0.eyJzdWIiOiJzIjM0ZDgycN02MmM5LTrmYUWtYYWny04NmjlYVlODRinZgjLCJhdQicloijjYWqtYxpZW50IiwiChJpbNpcGxLjoiyMzYNGQ4mjqtMzJjo802mFlLWE2MDctODziZW1tZtgYjwic4iwixXX0fa90aWll1joxjhjkMTAxnTawHdQ3LCJpc3MioliJQFgZq4yntcR7WRqZ10Jh1Pdv-2Uj-GAAT0u9GEWYyqBMrq0EwsOMn_yHGsZOWUxeBV1uBrvKjMSLB_AtbJj1PewcK1wv5jB1cLNhZCISInhjb381cyIGWjyvcGVuawQixSwiZXhWljoxNjkwTAzZm2AaLClJyQkiojE20TAxMDAs1gtR0HtLUFVVvgionsiYzXhaWlZijp7IKETWlPDo4YmLybwhes9nuZFLW7_44ad7CK9G1IA_T80yUgOnj6Qsyidc1BuSxw1WeemmMSDCA3-09PuG7RRMJZACxfa9L9HXdb_cq_yUM_bfQDewnuGr3B7lhndSw5D2Wtg
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36
9 Content-Type: application/json
0 Accept: application/json, text/plain, /*
1 X-Ghs-Auth: eyJhbGciOiJSUzIiNiIsImp0aSI6Ik1uWtVNREV3TVRvd01EUTB0enBoTmptaU9XWmxZbvJsiLwihLwjoiSlduIn0.evJzdWIiOiJzIjM0ZDgycN02MmM5LTrmYUWtYYWny04Nmjl

```

Response

| | | | |
|--------|-----|-----|--------|
| Pretty | Raw | Hex | Render |
|--------|-----|-----|--------|

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Credentials: true
3 Access-Control-Allow-Origin: https://cad-consumer-app-int.us-east.philips-healhtsuite.com
4 Access-Control-Expose-Headers: Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,Host,cache-control,content-type,content-transfer-encoding,Content-Type,Authorization,authorization,userid,edisp-introspect-value,Token,tken,Access-Control-Allow-Origin,Origin,X-GHS-AUTH,api-version,*
5 Cache-Control: no-cache, no-store
6 Content-Security-Policy: default-src 'self' *.philips-healhtsuite.com;
7 Content-Type: application/json
8 Date: Sun, 23 Jul 2023 08:49:56 GMT
9 Server: envoy
10 Strict-Transport-Security: max-age=63072000; includeSubDomains;
11 X-Envoy-Upstream-Service-Time: 54
12 X-Vcap-Request-Id: 534b3004-5ala-480f-76b2-4cff36c7d2c9
13 Connection: Close
14 Content-Length: 318192
15
16 {"id": "33b36708-2505-4e2-93d0-2034f76ecc62", "language": "en-us", "userId": "5619bf2-ff49-4739-956e-3f42bc773c8", "profileId": "2e2b3a65-5ebc-4014-838c-5ba22cb9096b", "profile": {"profileId": "2e2b3a65-5ebc-4014-838c-5ba22cb9096b", "userId": "5619bf2-ff49-4739-956e-3f42bc773c8", "identityId": "acbb1b49-8d92-46d2-b4c3-16af2cd8d5b1", "type": "CUSTODIAN", "lastLoggedIn": "1681806552, 663402000", "description": "Custodian Profile", "extendedAttributes": [{"attributeName": "CUSTODIAN_NAME", "attributeValue": "111110000"}, {"attributeName": "ORG_NAME", "attributeValue": "Philips"}, {"attributeName": "status", "attributeValue": "PENDING"}], "identity": {"id": "5619bf2-ff49-4739-956e-3f42bc773c8"}}, "resourceType": "OperationOutcome", "meta": {"created": "1690102318507", "lastUpdated": "1690102318507"}, "issue": [{"severity": "ERROR", "code": "GENERAL_ERROR", "diagnostics": "User is not authorized to access requested content"}]}

```

a. Actual request from admin user with 200ok response

Request

| | | | | |
|--------|-----|-----|----------------|-----------------|
| Pretty | Raw | Hex | JSON Web Token | JSON Web Tokens |
|--------|-----|-----|----------------|-----------------|

```

1 POST /identity/Search HTTP/1.1
2 Host: cad-api-gateway-int.us-east.philips-healhtsuite.com
3 Cookie: SESSION=91409590-114b-4f91-ae9f-08275b83975c
4 Content-Length: 43
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Mobile: ?0
7 Authorization: Bearer eyJhbGciOiJSUzIiNiIsImp0aSI6Ik1uWtVNREV3TVRvd01EUTB0enBoTmptaU9XWmxZbvJsiLwihLwjoiSlduIn0.eyJzdWIiOiJzIjM0ZDgycN02MmM5LTrmYUWtYYWny04NmjlOtgymMDkzZuiLCJhdQicloijjYWqtYxpZW50IiwiChJpbNpcGxLjoiyMzYNGQ4mjqtMzU0OS00GmyLtk5YIItMsACYjk4njASMCMLliwiYXV0a90aWll1joxjhjkMTAyMzAxMtzQwLCJpc3MioliJodHRwczpcLlwvGhpbiLwcy5jB1cLNhZCISInhjb381cyIGWjyvcGVuawQixSwiZXhWljoxNjkwTAzZm2AaLClJyQkiojE20TAxMDAs1gtR0HtLUFVVvgionsiYzXhaWlZijp7IKETWlPDo4YmLybwhes9nuZFLW7_44ad7CK9G1IA_T80yUgOnj6Qsyidc1BuSxw1WeemmMSDCA3-09PuG7RRMJZACxfa9L9HXdb_cq_yUM_bfQDewnuGr3B7lhndSw5D2Wtg
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36
9 Content-Type: application/json
0 Accept: application/json, text/plain, /*
1 X-Ghs-Auth: eyJhbGciOiJSUzIiNiIsImp0aSI6Ik1uWtVNREV3TVRvd01EUTB0enBoTmptaU9XWmxZbvJsiLwihLwjoiSlduIn0.evJzdWIiOiJzIjM0ZDgycN02MmM5LTrmYUWtYYWny04Nmjl

```

Response

| | | | |
|--------|-----|-----|--------|
| Pretty | Raw | Hex | Render |
|--------|-----|-----|--------|

```

1 HTTP/1.1 403 Forbidden
2 Access-Control-Allow-Credentials: true
3 Access-Control-Allow-Origin: https://cad-consumer-app-int.us-east.philips-healhtsuite.com
4 Access-Control-Expose-Headers: Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,Host,cache-control,content-type,content-transfer-encoding,Content-Type,Authorization,authorization,userid,edisp-introspect-value,Token,tken,Access-Control-Allow-Origin,Origin,X-GHS-AUTH,api-version,*
5 Cache-Control: no-cache, no-store
6 Content-Security-Policy: default-src 'self' *.philips-healhtsuite.com;
7 Content-Type: application/json
8 Date: Sun, 23 Jul 2023 08:51:58 GMT
9 Server: envoy
10 Strict-Transport-Security: max-age=63072000; includeSubDomains;
11 X-Envoy-Upstream-Service-Time: 9
12 X-Vcap-Request-Id: 0502d2ac-83d9-4cc9-4b09-26dd40383d45
13 Content-Length: 261
14 Connection: Close
15
16 {"id": "be4fb1c8-0276-4ef5-910b-f3bc39834d14", "resourceType": "OperationOutcome", "meta": {"created": "1690102318507", "lastUpdated": "1690102318507"}, "issue": [{"severity": "ERROR", "code": "GENERAL_ERROR", "diagnostics": "User is not authorized to access requested content"}]}

```

b. Same Request made by Custodian User with 403 Forbidden responses

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



7.9 Webapp/WebServices: Sensitive Information in URL

| | |
|-------------------------------|---|
| Vulnerability Title | Sensitive Information in URL |
| Vulnerability Category | A2 Cryptographic Failures |
| Severity | Low |
| CVSS V3 Calculation | CVSS Base Score: 3.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N |
| Description | <p><u>Vulnerability Description</u></p> <p>Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users. Ideally, HTTPS URLs despite encryption, are logged in plaintext in browser history, logs, trusted proxies, etc. The query string will be sent as part of the URL if the URL is passed to another site via the Referrer header. URLs sent to the user as part of an HTML page may be cached on disk.</p> <p>It is observed that EMAIL or Phone number and refresh token, code challenge are getting disclosed in URL.</p> <p>Reference: https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure</p> <p>Retest as of 24-July-2023: The issue is still Valid and not fixed.</p> <p>Retest as of 28-July-2023: The issue is fixed for Case 2. For the Case 1 issue is still valid and open.</p> <p><u>Exploitability rational</u></p> <p>An authenticated user of the application or an attacker who should be authenticated, can access this information by crawling the application across the functionalities. The attacker can gain this information from anywhere within the network. Potential access vectors may include but are not limited to:</p> <ul style="list-style-type: none"> • Browser history, proxy logs, web server logs, etc. • Shoulder-surfing the URL in a user's browser address bar. |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | |
|---------------------------------|--|
| | <p>Impact rational</p> <p>Exploitation of this scenario would allow attacker gather information as part of reconnaissance. Depending on the nature of the information, a malicious user may obtain personally identifiable information (PII), private user data or information which would allow user impersonation.</p> |
| Affected Systems/IP Address/URL | <p>https://cad-api-gateway-int.us-east.philips-healthsuite.com/oauth/token?grant_type=refresh_token&refresh_token=MTY4MTI5Nzk5NTg0Mjo0ODZhZjRINml4OnVzZXJuYW1lPTc2NTQzMjEwOTg6MTVkMDMzY2UzMzg3MjE1Y2NhMjY4ZWUxNzFlZjEwMDFjZGFiMGlzZmQzMjgyZWZjNjE1OGYyOWIxOGYxMDgzYzAzZjc5NGVhODRjNDdkOGRIZTlyZGRjZTE0MDcyNGlyZjVhYTY30DMzMmMzMjI5MDVIZTA2YTFjMzlzMmYzMmM=&client_id=cad-client</p> <p>https://cad-api-gateway-int.us-east.philips-healthsuite.com/oauth/authorize?response_type=code,token,id_token&scope=o penid&client_id=cad-client&redirect_uri=https://cad-consumer-app-int.us-east.philips-healthsuite.com&login_hint=EMAIL:chaitran.shivayogimath@philips.com&code_challenge=ZVeqsAYcKTEn1D_B4yl4vrcVmSHJ9QJ6GTkdXM_eR8&code_challenge_method=SHA256</p> <p>https://cad-consumer-app-int.us-east.philips-healthsuite.com/?code=97dd15307143a540818cf41950d1888ff78bc0120a4c8e9326&login_hint=cadadmin@grr.la</p> |
| Recommendation | <ul style="list-style-type: none"> It is recommended not to disclose internal identifiers like, variable names, system information, session information etc. Sensitive information should be sent using POST method only. <p>Reference: https://cheatsheetseries.owasp.org/cheatsheets/User_Privacy_Protection_Cheat_Sheet.html</p> |
| Status | Open (partially open for Case 1) |

Steps to Reproduce:

Step 1: Configure the browser to use a proxy tool such as Burp Suite.

Step 2: Intercept the request and observe that the sensitive information has been passed in the URL as shown in the below screenshot:

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Request

```
Pretty Raw Hex
POST /oauth/token?grant_type=refresh_token&refresh_token=
NTYwMTIwMjY0MjM0D0o0jJmJ1l0W710n1zZKJuW1Tk0p0TY50D4W16Nj3jNGE@0zc5ZTVjYTUhU
mEzzTgnWjg3zml0o0TkC0D1Y1T42GjyN2Z10WQ0YVYwUmU5Hm2h2R1HnUzUzDg000B1VjxNjgwYmf1HD
T3HNTdjhHmHmM7Q2zW51YThmHDU2jhNkewV0WUwMDBwDRhN0Mz0TA5NTdhYZAy%GzJhZc=&client_id=
cad-client HTTP/1.1
Host: cad-api-gateway-int.us-east.philips-healtsuite.com
Cookie: SESSION=30487b-41d0-45cf-ac0d-cf79971f13a5
Content-Length: 0
Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJhbGciOiJSUzIiNiItImp0aS16Ik1UWTRIVe13TpZHE5qTTF0am81W1FMk5tRmhLR1ppTwidH1wI
joiSi1dU1nb_eyJzDwI0i11m210fjQ2Y10mtg5L7QyHGI1T1TyOC0wNGH10TK32DawYz1lC3hdQ10i
JjYmQtY2xpZM50i1wchPbmhPcGx1TjoiHt01D10Hm1t10d40500fjR1UEyMjgtMDRjZTk5h2QwqGM
yJiwiXWY0af90aW11joNjigxMjAyHjQ2mU2Lcpc3H10jodRwcZpcL1wvcGhpbg6lwcyjb21z12h
ZC1sInHj3B1cyI6dyJvcGvuaWQixSw1ZKw1joxNjgxMjA0MDQ2LcpxQ10fje20DEyMDI2NDYs11gtR
0hTLUFVVEgi0ns1y2xha1zIjp7IKRFRKFTFQ1o1j9M950DUyNC030Gv2LTO5f1Q2tYjwv1o5H0DUzYT
A4HmW4Yjif5ws1dxN1ck1kj1o1ntdiH10m1t10d40500fjR1UEyMjgtMDRjZTk5h2QwqGMlyIn0sImp
0aS161k1UMTRIVe13TpZHE5qTTF0am81W1FMk5tRmhLR1ppTwidH1yXV0aG9yAxRpZX10i1ERUZBVUxU
In0t.phrZT630epx4aqFXU3Tw6hvBe2vTXMuxuX6PYMKhewBK-1RQ1VGm5v/R3Jk4jrrmk0UjaBa
4GozhipIn3u2st01q7d0ndll7dsRT9ySEB1kFHR841eOxbAGvvYFLPg_QatVdu0ubizkYHbf71a
Content-Type: application/json
Date: Tue, 11 Apr 2023 08:49:44 GMT
Referer-Policy: no-referrer
Server: envoy
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Envoy-Upstream-Service-Time: 118
X-Frame-Options: DENY
X-Vcap-Request-Id: f4fa5f6a-30f8-4950-603c-3f3b7a0c1adb
Content-Length: 2433
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Credentials: true
3 Access-Control-Allow-Origin: https://cad-consumer-app-int.us-east.philips-healtsuite.com
4 Access-Control-Expose-Headers: Accept,Accept-encoding,Connection,Content-Length,keep-alive,user-agent,Host,cache-control,content-type,content-transfer-encoding,Content-Type,Authorization,authorization,userid,edisp-introspect-value,Token,token,Access-Control-Allow-Origin,Origin,X-GHS-AUTH,api-version,*
5 Cache-Control: no-cache
6 Content-Type: application/json
7 Date: Tue, 11 Apr 2023 08:49:44 GMT
8 Referer-Policy: no-referrer
9 Server: envoy
10 Strict-Transport-Security: max-age=31536000 ; includeSubDomains
11 X-Content-Type-Options: nosniff
12 X-Envoy-Upstream-Service-Time: 118
13 X-Frame-Options: DENY
14 X-Vcap-Request-Id: f4fa5f6a-30f8-4950-603c-3f3b7a0c1adb
15 X-Xss-Protection: 1 ; mode=block
16 Content-Length: 2433
```

Refresh token getting disclosed in URL

Request to <https://cad-api-gateway-int.us-east.philips-healtsuite.com:443> [34.195.19.186]

| | | | | |
|---------|------|-----------------|--------|--------------|
| Forward | Drop | Intercept is on | Action | Open browser |
|---------|------|-----------------|--------|--------------|

```
Pretty Raw Hex
1 GET /oauth/authorize?response_type=code_token,id_token&scope=openid&client_id=cad-client&redirect_uri=https://cad-consumer-app-int.us-east.philips-healtsuite.com&
logInHint=PHONE:7376149524&code_challenge=3XZpSVxe4HEaSLHVsXul5Kall7RCEcQ8yftxcPhyUDU&code_challenge_method=SHA256 HTTP/1.1
2 Host: cad-api-gateway-int.us-east.philips-healtsuite.com
3 Cookie: SESSION=
4 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
0 Sec-Fetch-Site: same-site
1 Sec-Fetch-User: ?1
2 Sec-Fetch-Dest: document
3 Referrer: https://cad-consumer-app-int.us-east.philips-healtsuite.com/
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-US,en;q=0.9
7 Connection: close
8
```

Phone number getting disclosed in URL

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Case 1:

Retest Status as of 24th July 2023

The screenshot shows a NetworkMiner interface with two main sections: 'Request' and 'Response'.
Request:
HTTP/1.1 200 OK
Cache-Control: no-cache, must-revalidate
Content-Type: text/html
Date: Sat, 22 Jul 2023 04:15:29 GMT
Etag: W/"64b503eb-abad"
Last-Modified: Mon, 17 Jul 2023 09:03:39 GMT
Server: nginx
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Vcap-Request-ID: a75b9768-9c55-4054-5b9d-62e9d0f1fb28
X-Xss-Protection: 1; mode=block
Connection: Close
Content-Length: 2701

16 <!doctype html><html lang="en">
 <head>
 <meta charset="utf-8"/>
 <link rel="icon" href=".//favicon.ico"/>
 <meta name="viewport" content="width=device-width,initial-scale=1,viewport-fit=cover"/>
 <meta name="description" content="Guided Health Services"/>

Response:
HTTP/1.1 200 OK
Cache-Control: no-cache, must-revalidate
Content-Type: text/html
Date: Sat, 22 Jul 2023 04:15:29 GMT
Etag: W/"64b503eb-abad"
Last-Modified: Mon, 17 Jul 2023 09:03:39 GMT
Server: nginx
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Vcap-Request-ID: a75b9768-9c55-4054-5b9d-62e9d0f1fb28
X-Xss-Protection: 1; mode=block
Connection: Close
Content-Length: 2701

Email ID is visible under url

Case 2:

Test Evidence as of on 24 July 2023:

The screenshot displays the Postman application interface. On the left, the 'Request' tab is active, showing a GET request to `/engagement/report?reportStartDate=2023-07-14T10:22:38Z&reportEndDate=2023-07-14T10:22:38Z&reportType=BEATS`. The 'Response' tab is also visible, detailing the HTTP response with status code 200 OK, various headers like Access-Control-Allow-Origin, and a JSON response body containing engagement data. The right side of the interface includes an 'Inspector' panel with sections for Request attributes, Request query parameters, Request cookies, Request headers, and Response headers.

Sensitive information disclosed

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Retest Evidence as of on 28 July 2023:

Target: <https://cad api gateway-int.us-east.philips-healtsuite.com>

Request

```
Send Cancel < > < >
```

Pretty Raw In Actions ▾

Response

Pretty Raw Render In Actions ▾

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Credentials: true
3 Access-Control-Allow-Origin: https://cad-consumer-app-int.us-east.philips-healtsuite.com
4 Access-Control-Expose-Headers: Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,Host
5 Cache-Control: no-cache,no-store
6 Content-Type: application/json
7 Date: Fri, 28 Jul 2023 10:10:56 GMT
8 Server: envoy
9 Strict-Transport-Security: max-age=8725000; includeSubDomains;
10 X-Envoy-Request-Time: 28
11 X-Envoy-Request-Id: 501efad6-0eaa-4e30-53ae-0c51733d5ce0
12 X-Trace-Request-Id: 501efad6-0eaa-4e30-53ae-0c51733d5ce0
13 Content-Length: 19790
14 Connection: Close
15 {
16   "startDate": "2023-07-14T10:00:30Z",
17   "endDate": "2023-07-14T14:22:30Z",
18   "name": null,
19   "reportDate": "2023-07-14T14:22:34.192410Z",
20   "age": 43,
21   "gender": "male",
22   "height": 177.16,
23   "mass": 84.0,
24   "email": "37.7401303459945C04",
25   "location": null,
26   "type": "BEATS",
27   "beatScore": 34.192410Z,
28   "beatScoreValue": 3.340666930048263,
29   "beatScoreInterpretation": "3",
30   "summary": null,
31   "pf": [
32     {
33       "Extreme_RHR_PF_Statement": "Extreme_RHR_PF_Statement",
34       "Extreme_BP_PF_Statement": "Extreme_BP_PF_Statement",
35       "Emotional_EHR_PF_Statement": "Emotional_EHR_PF_Statement",
36       "Emotional_EBPV_PF_Statement": "Emotional_EBPV_PF_Statement"
37     },
38     {
39       "ClinicalLab_GRA_BP_Statement": "ClinicalLab_GRA_BP_Statement",
40       "Emotional_EI_BP_Statement": "Emotional_EI_BP_Statement"
41     }
42   ],
43   "original": "https://cad-consumer-app-int.us-east.philips-healtsuite.com",
44   "server": "https://cad-consumer-app-int.us-east.philips-healtsuite.com",
45   "size": 16634 bytes | 553 millis
46 }
```

Activate Windows
Go to Settings to activate Windows

Done

Sensitive information is not visible and fixed in next build

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



7.10 Webapp: Misconfigured CORS

| | |
|-------------------------------|---|
| Vulnerability Title | Misconfigured CORS |
| Vulnerability Category | A5 Security Misconfiguration |
| Severity | Low |
| CVSS V3 Calculation | CVSS Base Score: 3.1 CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N |
| Description | <p>Vulnerability Description:</p> <p>During security assessment it is observed that the server is configured with an unrestricted HTML5 Cross-Origin Resource Sharing (CORS) policy. CORS defines whether resources on other domains can interact with this server. An attacker can place malicious JavaScript on his domain that can exploit the unrestrictive CORS policy to access sensitive data on this server or perform sensitive operations without the user's knowledge. Additionally, an attacker could exploit security vulnerabilities on other domains to compromise services on this server. The CORS policy relaxes the Same Origin Policy, an important security control that isolates potentially malicious resources to its respective domain name.</p> <p>If a script attempts to violate the Same Origin Policy by interacting with another domain, modern browsers can check a server's CORS policy by issuing a "pre-flight request". The browser allows the interaction only if the server responds with an Access-Control-Allow-Origin header that lists the script's domain or a wildcard match (*). A wildcard match allows interaction from any other domain, which allows any malicious content to retrieve content from this server or perform user actions.</p> <p>Retest status(17/April/2023):</p> <p>It is observed that CORS Misconfiguration is still not rectified. Hence the issue is OPEN.</p> <p>Retest status (26/April/2023):</p> <p>It is observed that CORS Misconfiguration has been rectified. Hence marking this issue as CLOSED.</p> <p>Retest status (24/July/2023):</p> <p>Issue has been fixed.</p> |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | |
|---------------------------------|---|
| | <p>Exploitability Rational: An unrestricted CORS policy allows an attacker to access sensitive data or perform unauthorized user actions without user knowledge. Malicious JavaScript can perform these actions even if the server uses Cross Site Request Forgery tokens.</p> <p>Impact Rational: An attacker can access sensitive data of victim. An unrestricted CORS policy allows an attacker to access sensitive data or perform unauthorized user actions without user knowledge.</p> <p>https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_(OTG-CLIENT-007)</p> |
| Affected Systems/IP Address/URL | <p>https://cad-api-gateway-staging.us-east.philips-healthsuite.com/phr?subject=bbaa6ab0-9832-4b31-bb23-9d5fad8b90cc&sort=-effectiveDateTime&count=1&category=ehi</p> <p><i>Note: This is an issue with entire application endpoints. Instances are not limited to the above items. Fix should be applied across the collection.</i></p> |
| Recommendation | The Access-Control-Allow-Origin header should not be set to a wildcard match. In most cases, this header can be safely removed. If the application requires a relaxation of the Same Origin Policy, the AccessControl-Allow-Origin header should whitelist only domains that are trusted by this server. Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains. |
| Status | Closed |



Supportive Evidence:

Request

```
Pretty Raw Hex ⌂ V | 
1 POST /ehr/api/patient/v1 HTTP/1.1
2 Host: cad-api-gateway-int.us-east.philips-healthsuite.com
3 Cookie: SESSION=f949576-d594-4680-822e-7a799a09930e
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.9
7 Accept-Encoding: gzip, deflate
8 Referer: https://cad-consumer-app-int.us-east.philips-healthsuite.com/
9 Content-Type: application/json
10 User-Agent: curl/7.61.1
11 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJsb2dpbiI6ImFkbWluLmNvZGluZG93bmxvY2F0aW9ucyIsInR5cGUiOiJsb2dpbiJ9.eyJzdWIiOiJ0ZXJtZW5zaWQxMjI0ZTB10TQ5ZWY1CJhdHQjQ1oi
12 j3jWYQtY2xpZMs0iiviciH2pbmllpcGx1IjoxMTkzMQ4zYtZjRiY100fjA4lTk3YTAtHzYtNGwzTkpd0WV
13 nIxIyXV0IjoxM0aW1IjoxHjgx0Dg0DAwD40LC3pc3hioioidHRwcpc1lwvcGhb61wcy5jb21cl2Nh
14 ZC3Injb3b1c1y16hlyjcvGvualQIXSw1ZhmeIjoxHjgx0Dg2HjAwLcJpYXQi0je20DE40D4HdAs1lgtr
15 0hTLUFVVEgi0ns1YxNaH1zTj7p7KmPT1MVUTStj01nRjY21YtCtzD0U500fDbalThkYzgtZGU4Ym
16 VjZGHNH2z1In0n1vz2X3j2C161jeyzGZk0GzLmUV0wItNDImOC05H2eWlThlyjR1HUG5H0D112j39Lc3
17 qdGk101jMVfk0TV/RnNE5E23dlREF3TkrkveUrtBzak14lWp3j)IsIm1dGhvcma0hVtj0iQ090U1Vh
18 RVi1FQ_pyLc3w1bTF_x_H6epH8ggVzjYiF7rTUoUifer0HqDeD56h7_FMBRrqUp2_gotFDIx0z644A
19 WHu2n9CS5m8FbexTSvHuISvVtYcmHjV083caaty9hidKArlA16wvd20Pnzb412P_mH1372BLlCpvg
20 ALJv726pR6qbzy_eq3x1as1btKuePjcg8v02lV3c6h0J112DUA-V203LYtRcf2Bz0Uqnzoqj1e9267j-
21 1L0XF7lqqcAxmat3huFLHs3jQpJZ58tB7jnRAhfTAVDzYafQCrFzRaSxDJxm578D6bd1Hf15Hfz
22 z18PwCjfuKIJ8F44C4Kcfykg
23 
24 Api-Version: 1
25 Sec-Ch-Ua-DistForm: "Windows"
26 Origin: https://evil.com
27 Sec-Fetch-Site: same-site
28 Sec-Fetch-Mode: cors
29 Sec-Fetch-Dest: empty
30 Referer: https://cad-consumer-app-int.us-east.philips-healthsuite.com/
31 Accept-Encoding: gzip, deflate
32 Accept-Language: en-US,en;q=0.9
33 If-None-Match: W/"1480-1wktVsGOKRD5bNmK7V2GkDq4"
34 Connection: close
35 
```

Response

```
Pretty Raw Hex ⌂ V | 
1 Access-Control-Allow-Credentials: true
2 Access-Control-Allow-Origin: https://evil.com
3 Date: Mon, 12 Dec 2022 04:53:36 GMT
4 Server: Apache/2.4.41 (Ubuntu)
5 X-Envoy-Upstream-Service-Time: 4
6 X-Vcap-Request-Id: ce790ba9-2109-4fe9-616b-c17f6324fa70
7 Content-Length: 11
8 Connection: Close
9 
10 
11 
```

Retest status as of 17 April, 2023:

Request

```
Pretty Raw Hex ⌂ V | 
1 POST /ehr/api/patient/v1 HTTP/1.1
2 Host: cad-api-gateway-int.us-east.philips-healthsuite.com
3 Cookie: SESSION=f949576-d594-4680-822e-7a799a09930e
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.9
7 Accept-Encoding: gzip, deflate
8 Referer: https://cad-consumer-app-int.us-east.philips-healthsuite.com/
9 Content-Type: application/json
10 User-Agent: curl/7.61.1
11 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJsb2dpbiI6ImFkbWluLmNvZGluZG93bmxvY2F0aW9ucyIsInR5cGUiOiJsb2dpbiJ9.eyJzdWIiOiJ0ZXJtZW5zaWQxMjI0ZTB10TQ5ZWY1CJhdHQjQ1oi
12 j3jWYQtY2xpZMs0iiviciH2pbmllpcGx1IjoxMTkzMQ4zYtZjRiY100fjA4lTk3YTAtHzYtNGwzTkpd0WV
13 nIxIyXV0IjoxM0aW1IjoxHjgx0Dg0DAwD40LC3pc3hioioidHRwcpc1lwvcGhb61wcy5jb21cl2Nh
14 ZC3Injb3b1c1y16hlyjcvGvualQIXSw1ZhmeIjoxHjgx0Dg2HjAwLcJpYXQi0je20DE40D4HdAs1lgtr
15 0hTLUFVVEgi0ns1YxNaH1zTj7p7KmPT1MVUTStj01nRjY21YtCtzD0U500fDbalThkYzgtZGU4Ym
16 VjZGHNH2z1In0n1vz2X3j2C161jeyzGZk0GzLmUV0wItNDImOC05H2eWlThlyjR1HUG5H0D112j39Lc3
17 qdGk101jMVfk0TV/RnNE5E23dlREF3TkrkveUrtBzak14lWp3j)IsIm1dGhvcma0hVtj0iQ090U1Vh
18 RVi1FQ_pyLc3w1bTF_x_H6epH8ggVzjYiF7rTUoUifer0HqDeD56h7_FMBRrqUp2_gotFDIx0z644A
19 WHu2n9CS5m8FbexTSvHuISvVtYcmHjV083caaty9hidKArlA16wvd20Pnzb412P_mH1372BLlCpvg
20 ALJv726pR6qbzy_eq3x1as1btKuePjcg8v02lV3c6h0J112DUA-V203LYtRcf2Bz0Uqnzoqj1e9267j-
21 1L0XF7lqqcAxmat3huFLHs3jQpJZ58tB7jnRAhfTAVDzYafQCrFzRaSxDJxm578D6bd1Hf15Hfz
22 z18PwCjfuKIJ8F44C4Kcfykg
23 
24 Api-Version: 1
25 Sec-Ch-Ua-DistForm: "Windows"
26 Origin: https://evil.com
27 Sec-Fetch-Site: same-site
28 Sec-Fetch-Mode: cors
29 Sec-Fetch-Dest: empty
30 Referer: https://cad-consumer-app-int.us-east.philips-healthsuite.com/
31 Accept-Encoding: gzip, deflate
32 Accept-Language: en-US,en;q=0.9
33 If-None-Match: W/"1480-1wktVsGOKRD5bNmK7V2GkDq4"
34 Connection: close
35 
```

Response

```
Pretty Raw Hex ⌂ V | 
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Credentials: true
3 Access-Control-Allow-Origin: https://evil.com
4 Access-Control-Expose-Headers: 
5 Accept,Accept-Encoding,Content-Length,keep-alive,user-agent,Host,cache-control,content-type,content-transfer-encoding,Content-Type,Authorization,authorization,userid,edisp,introspect-value,Token,token,Access-Control-Allow-Origin,origin,X-GHS-AUTH,api-version,*
6 Content-Type: application/fhir+json; charset=utf-8
7 Date: Wed, 19 Apr 2023 06:35:34 GMT
8 Etag: W/"1480-phfvCqcrqrf6/W/Bs84yu79j"c
9 Server: envoy
10 X-Envoy-Upstream-Service-Time: 37
11 Content-Length: 5248
12 Connection: Close
13 
14 {
15   "resourceType": "Bundle",
16   "id": "2014d744-c76f-4538-91b1-61acb3d374d86",
17   "meta": {
18     "lastUpdated": "2023-04-19T06:35:34.946Z"
19   },
20   "type": "searchset",
21   "url": "https://cad-api-gateway-int.us-east.philips-healthsuite.com/ehr/api/patient/v1?patient=1&_format=json"
22 } 
```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Retest status as of 26 April, 2023:

Target: <https://cad-api-gateway-staging.us-east.philips-healthsuite.com>

| Request | Response |
|--|--|
| <pre>Pretty Raw Hex joiS1dIn0.eyJzdiI0JiYmFhImFiC050DhylTRiMz:etwIy05ZDVwYQ4YjkxY2HlCJhdQj0i jYQWQY2xp2WS01iiciH3pbmllpcGxLJjoxYmJHYT2HjYAt0tgzH00YjMxLWJhjMjtOWQ1zfkdG15f6H jTiwVYXV0af90W11TjoxHjgjyHTz=H2f5HDf4L3pc3H0i3odHkewcp1lwvGhpBGlwcy5jb21c12H ZC1sInhjB3B1cyI6WjYvcGVuaQ0iXSw1ZkhmIjoxHjgjyHTA1NT5L3pYXQj0jE20D1IMDf3H2ks1LgtR 0HtLUFVVEgi0nsiY2xhM1zTjz7TkHPT1HVTUvS2jjoiTgwZGV40dEtN2210C000WR1MEy2DfHjdwYz H10WQyyzBk1nbsInvzZJ32C161w31vNE2W1nslTkd2ItNG1zMS1jY1z1TlkHWzhDhiOTbjYy39LcJ odgk1o1JhVfk0Tpvd0l6Y3opVFf6T0RvNU16RTVW1kvwm1HHS1sImf1dGhvcml0mVv:zjoi0909U1VH PV1jFQ_UNlZ06v9aQuarntHg2f8n5_Seb0ohT20kVqHhb:ajF41fkIaasjt43pKncsY162HkP3CHU 7IL1RT-kko5v6/k0D511mQH7bsH10c52basevN4GHmx_M7zlpQ6klaejdn-VnA9rluf7iqb32GX3 r2CRk2HLH1Td3-LTb1t50m0512notGS1hejurWqggf7bnj3o_Qc_xAZ9r5oXzileSSs-0hQ0a-XUY_vt h75s3I6ngvBVwkrn63eUUh:TYjmq0mrj6vD1GzdeKA3hsxt18vjq1c20FO_xIGbiPca1vxfsbE1C nvxFdf_Sss0qrccZIKuZneQ 11 Api-Version: 1 12 Sec-Ch-Ua-Platform: "Windows" 13 Origin: https://evil.com 14 Sec-Fetch-Site: sameSite 15 Sec-Fetch-Mode: cors 16 Sec-Fetch-Dest: empty 17 Referer: https://cad-consumer-app-staging.us-east.philips-healthsuite.com/ 18 Accept-Encoding: gzip, deflate 19 Accept-Language: en-US, en;q=0.9 20 If-None-Match: W/"134-0TAvtXF93yvUqr7k6z15oLv+hM" 21 Connection: close 22 23</pre> | <pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Content-Type: application/fhir+json; charset=utf-8 3 Date: Wed, 26 Apr 2023 10:09:28 GMT 4 Etag: W/"134-1B1hCwbMUmhKyrYxZq165sGK970" 5 Server: envoy 6 X-Envoy-Upstream-Service-Time: 47 7 X-Vcap-Request-Id: 76ca87d8-bfeb-4471-7919-03525813bab6 8 Content-Length: 308 9 Connection: Close 10 11 { "resourceType": "Bundle", "id": "e4413c94-e7e2-4233-9665-d9483928b7c8", "meta": { "lastUpdated": "2023-04-26T10:09:28.107Z" }, "type": "searchset", "total": 0, "link": [{ "relation": "self", "url": "https://API_URL.com?subject=bbaa6ab0-9832-4b31-bb23-9d5fad8b90cc&_sort=-effectiveDateTime&_count=1&category=ehi" }] }</pre> |

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



7.11 Webapp/WebServices: HTTPS Fallback Allowed

| | |
|---------------------------------|---|
| Vulnerability Title | HTTPS Fallback Allowed |
| Vulnerability Category | A5 Security Misconfiguration |
| Severity | Low |
| CVSS V3 Calculation | CVSS Base Score: 3.1 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N |
| Description | <p>Vulnerability Description: During the assessment, it was observed that the below mentioned endpoints supported HTTP as well. By default, API's are served in HTTPS, but the connection can be downgraded to HTTP.</p> <p>Retest status(17/April/2023):</p> <p>It was observed that the issue persists for some domains.</p> <p>Retest as of 24-July-2023: The issue is still Valid and not fixed.</p> <p>Exploitability Rational: If a victim accesses the application with an HTTP-based URL, an attacker listening on any network between the victim and the application server may view and modify application traffic.</p> <p>Impact Rational: Attacker can perform Man in the middle attack also can see all communication in clear text</p> |
| Affected Systems/IP Address/URL | http://cad-consumer-app-int.us-east.philips-healthsuite.com/ https://cad-cardiovital-app-int.us-east.philips-healthsuite.com/ WebService Endpoint: https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report |
| Recommendation | <ul style="list-style-type: none"> HTTPS should be enabled and enforced on the application server. Once HTTPS has been properly configured, ensure that the application requires HTTPS for access to all application resources, including JavaScript files, style sheets, and images. When a user attempts to navigate to any part of the application over HTTP, the application should redirect the user to the HTTPS version of the application. |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | |
|--------|--|
| | <ul style="list-style-type: none"> it is recommended that applications are deployed with HTTP Strict Transport Security (HSTS). HSTS forces the browser to access a site only over HTTPS and prevents access in cases where the authenticity of the X.509 certificate cannot be verified. HSTS is supported in recent versions of the Chrome, Firefox, and Opera web browsers. To enable HSTS, simply add the Strict-Transport-Security header to the response header when users first access the site over HTTPS. <p>References:</p> <ul style="list-style-type: none"> https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security |
| Status | Open |

Steps to Reproduce

Step1: Capture the application request in Burp, which is running on port 443.

Step2: Now click on the target bar and uncheck the https, upon sending the request with port 80, a proper response captured as shown below screenshots.

```

Request
Pretty Raw Hex Query Params
1 GET /signin HTTP/1.1
2 Host: cad-consumer-app-int.us-east.philips-healhtsuite.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Te: trailers
13 Connection: close
14
15

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Content-Type: text/html
3 Content-Length: 2534
4 Date: Fri, 15 Dec 2022 05:34:58 GMT
5 Etag: "639e79fb-9e6"
6 Last-Modified: Thu, 15 Dec 2022 19:09:47 GMT
7 Server: nginx/1.22.1
8 X-Vcap-Request-Id: 9e7a9628-b406-412f-61e0-7c1dbaa0ea0a
9 Content-Length: 2534
10 Connection: Close
11
12 <!doctype html><html lang="en">
<head>
<meta charset="utf-8"/>
<link rel="icon" href="/favicon.ico"/>
<meta name="viewport" content="width=device-width,initial-scale=1,viewport-fit=cover"/>
<meta name="theme-color" content="#5F9920"/>
<meta name="description" content="Guide Health Services"/>
<link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png"/>
<link rel="icon" type="image/png" sizes="32x32" href="/favicon-32x32.png"/>
<link rel="icon" type="image/png" sizes="16x16" href="/favicon-16x16.png"/>
<link rel="apple-touch-startup-image" href="/splashScreen-640x1136.png" media="(&device-width: 320px) and (&device-height: 560px) and (-webkit-device-pixel-ratio: 2) and (orientation: portrait)">
<link rel="apple-touch-startup-image" href="/splashScreen-750x1334.png" media="(&device-width: 375px) and (&device-height: 667px) and (-webkit-device-pixel-ratio: 2) and (orientation: portrait)">
<link rel="apple-touch-startup-image" href="/splashScreen-1242x2208.png" media="(&device-width: 414px) and (&device-height: 736px) and (-webkit-device-pixel-ratio: 3) and (orientation: portrait)">
```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Retest status as of 17/April/2023:

The screenshot shows the Postman interface with two main panels: 'Request' and 'Response'. The 'Request' panel contains a raw HTTP message:

```
1 GET /index.html HTTP/1.1
2 Host: cad-consumer-app-int.us-east.philips-healtsuite.com
3 Cookie: SESSION=23796e18-b0fb-424b-9468-b6b143bf763c
4 Pragma: no-cache
5 Cache-Control: no-cache
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
7 Accept: /*
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: cors
10 Sec-Fetch-Dest: empty
11 Referer: https://cad-consumer-app-int.us-east.philips-healtsuite.com/index.html
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US, en;q=0.9
14 Connection: close
```

The 'Response' panel shows the server's response:

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, must-revalidate
3 Content-Type: text/html
4 Date: Tue, 11 Apr 2023 06:15:44 GMT
5 Etag: W/"64343b18-9d8"
6 Last-Modified: Mon, 10 Apr 2023 16:36:40 GMT
7 Server: nginx/1.22.1
8 Vary: Accept-Encoding
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Request-ID: 8b5b164b-4f40-45f9-6ab3-c3fc88c68834
12 X-XSS-Protection: 1; mode=block
13 Connection: Close
14 Content-Length: 2520

doctype html><html lang="en">
<head>
<meta charset="utf-8"/>
<link rel="icon" href=".//favicon.ico"/>
<meta name="viewport" content="width=device-width, initial-scale=1, viewport-fit=cover"/>
<meta name="description" content="Guided Health Services"/>
<link rel="apple-touch-icon" sizes="180x180" href=".//apple-touch-icon.png"/>
<link rel="icon" type="image/png" sizes="32x32" href=".//favicon-32x32.png"/>
<link rel="icon" type="image/png" sizes="16x16" href=".//favicon-16x16.png"/>
```

A modal window titled 'Configure target details' is open in the center, prompting for 'Host' (app-int.us-east.philips-healtsuite.com), 'Port' (80), and 'Use HTTPS' (unchecked). At the bottom of the modal are 'OK' and 'Cancel' buttons.

PHILIPS SCOF

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Send Cancel < > [Search...](#) 0 matches

Target: <http://cad-cardiovital-app-int.us-east.philips-healthsuite.com> HTTP/1.1

| Request | | Response | |
|---|---|----------|-----|
| Pretty | Raw | Pretty | Raw |
| 1 / HTTP/1.1 | 1 HTTP/1.1 200 OK | | |
| 2 Host: cad-cardiovital-app-int.us-east.philips-healthsuite.com | 2 Accept-Ranges: bytes | | |
| 3 Cookie: SESSION=4118697-8558-4538-9258149; encryptedMessage=JU2f5dsk0Q19bhy-vkTUbrcI5e9atwdstD13fxBdrn0fE28Kw1jdtdq2c>IxHwfxtKD1B81vBbW%2F11gpg2B21Y1VBY1C1NxSv07z2f2An28j12Bpx2B2zT1QjUghx2B2Dx1sfD0g1C1T6Vb/00v1fNYCk2Bn2Fc1xGx-CR1a2zC5l93hGt1VCzAfkH7H36r1qng4d8cb5h5E9pJbd0jyqysHVEldc8GyWmVv1y18ajp23J1ICU0H2BPM142FAAX6fVD/RQZp1TCU4%2B0%Uglabtg2L1rTfG40pma7Af0xsa1UPOCoQf9K3CN2B6u2z-Df1mz59j1n42zBQa1h1t-FvA2B2zTSPV2ghoFimby-UdPfFU02b6kh9d7zBh10fC0f0gauhmn2f1wv+ah5Mhp0cGz50t%551xQpaRA4B1h1pDfIt2cf2r4V%4F2CHe19j3jy1ZjCjkhNUH6UtonQzF1Cd0eCoAr67k3C6nL2fUN2B2qf1H3jrgjB4B1XV2f1wsgROXu5153v9hdh-aewPmg1Um9Q200TDEoawB2D4Hls%Q2F2B2gpkH0jIGT1R7rARveorgk1z2B1jUHw2B7S17yxDrnxmz2D1bKt1XD1R0t0nQzF1Cd0eCoAr67k3C6nL2fUN2B2qf1H3jrgjB4B1XV2f1wsgROXu5153v9hdh-s03s5cofcauf0l51ahauH79CVAh7dEPjgqv9c4%2B2BKzKchkuFuUHnf2tQ067F2ambRhlv+vwBkm1K1v2X168KtUkxDkIAu1JH37ZopTbg3RusJ8g>c2B6g52FxVpQduQdYCrYz-Pso-yPfA10uH87R0t1KtCkoaujw190225%2F6m0Bnqc1a1qzYSuSD4f1tB4T1M2B8pHd73d0uB18g9mrsJAc1wNz2B2L02HtrfHtr7agPn0lxFU7x2BYF1VpugkP667QWmAn0zX1jpl7Ty6gcH0UyV0j1av0/PVxqz52B7Cq059Cp9S5hBmI6C1OT1V39pdk60d3C10f0d0uhs028B1c3a0s2Qrtgvslgn961tBlnPkkcg2B51Y3hrAqqjx2f1M54d1l28d8j0lzp1jTBS5B2B6H6P215jB1zCJDNW1ktD2znoh1ne941al.WB1PQ0582f6P1lIned2P3oTmc51Gdrvnu0zKw2B7V9n10z6C1MDf1xPms35F2zUpdHJ095val.0f5kxMeD0f6B2f8z2K1c5g9jw8Bge14efamQhgrkQ1griqyE0yhsbl2gUYyV1kygg1tCq0Z7j2f1jK2f1TdphK9y1fdDc4h61ly1Bjfbhjdtptw0zT2B2K2Wb1ja0rUfjqlqy532h9gZ57T03E3EWb2B2tHjw5z0n0gecck2B0t71L7kf18tabhQuqh12D1n62G2C7jB2Ezyg566p1fB2ezhvLB00AHm1qD0s0RpeYmawAxCu46QuaJh6FRxxjCeavHxkBo1x2bdYQgb2wb131K1f1qz2B0DewpwhG | 3 Cache-Control: no-store, no-cache, must-revalidate | | |
| 4 Content-Type: text/html | 4 Content-Type: text/html | | |
| 5 Date: Tue, 11 Apr 2023 09:08:34 GMT | 5 Date: Mon, 10 Apr 2023 12:59:45 GMT | | |
| 6 Etag: "64340841-2f6" | 6 Etag: "64340841-2f6" | | |
| 7 Last-Modified: Mon, 10 Apr 2023 12:59:45 GMT | 7 Last-Modified: Mon, 10 Apr 2023 12:59:45 GMT | | |
| 8 Server: nginx/1.22.1 | 8 Server: nginx/1.22.1 | | |
| 9 X-Content-Type-Options: nosniff | 9 X-Content-Type-Options: nosniff | | |
| 10 X-Frame-Options: SAMEORIGIN | 10 X-Frame-Options: SAMEORIGIN | | |
| 11 X-Vcap-Request-Id: 8a93c795-32-46c1-4f9d-e0dec871511e | 11 X-Vcap-Request-Id: 8a93c795-32-46c1-4f9d-e0dec871511e | | |
| 12 X-Xss-Protection: 1; mode=block | 12 X-Xss-Protection: 1; mode=block | | |
| 13 Content-Length: 758 | 13 Content-Length: 758 | | |
| 14 Connection: Close | 14 Connection: Close | | |
| 15 | 15 | | |
| 16 <!doctype html><html lang="en"> | 16 <!doctype html><html lang="en"> | | |
| <head> | <head> | | |
| <meta charset="utf-8"/> | <meta charset="utf-8"/> | | |
| <link rel="icon" href="/favicon.ico"/> | <link rel="icon" href="/favicon.ico"/> | | |
| <meta name="viewport" content="width=device-width, minimum-scale=1, maximum-scale=1, initial-scale=1, viewPort-fit='cover'"/> | <meta name="viewport" content="width=device-width, minimum-scale=1, maximum-scale=1, initial-scale=1, viewPort-fit='cover'"/> | | |
| <meta name="theme-color" content="#000000"/> | <meta name="theme-color" content="#000000"/> | | |
| </head> | </head> | | |
| <body> | <body> | | |
| <div> | <div> | | |
| </div> | </div> | | |
| </body> | </body> | | |
| </html> | </html> | | |

 < > [Search...](#) 0 matches

 < > [Search...](#) 0 matches



Request

Pretty Raw Hex

1 GET /phr?subject=12fdf8ff-f4bb-4208-97a0-3224e0e949ef&_sort=-effectiveDateTime&_count=1&category=ehi-sector HTTP/1.1

2 Host: cad-api-gateway-int.us-east.philips-healthsuite.com

3 Cookie: SESSIONID=84536ff-8200-4e91-bf6b-783c576b43a5

4 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="112"

5 Edisip-Introspect-Value:
eyJhY3RpdmU2dnYydnUsInVzZXJ0Ym1IjozTA00W13MDItMzhjYt00Hg1LTw0tjYtNTUy0Th1N2ZIMj1Ii1w1c3V1ij0zDE2EzH1kYyktzJ4A4H1000zJ1lWF1N2HtMhU4Dzg=M20Um0UzIwiw1KzIjoiaHRhC8hM6Ly9jWQctCHzYnVpbGQduX0WZfzd5waGisAxBzLWh1Vx0AH1x1R1mlwv5p9Y0wYXV0a90b2t1biIsIm4C16M7YMTc0TM4wiwb1WfUyVdpbpmDPCmhdbm16YXRpBz4S01X1MjAzK0dMhT1klTQ1ZGET0tgSMC00Vh1WtU4ZDwYzA1LcJvcmdhbm16YXRpBz52C16IjeYfDfklM0TA10W0HDVY50050dkh1TE=tHueXtHnk1bjBMCIsInJvB2V1jpbIKHPT1WtUV1S119KSwdg9rZWSfdHlwZS16IkJY1J1cIsImk1Zw50aR5X3R5Gu0i1c2V1ywidg9rZWSfdHlwZ99aU07ojoYm1jZXNzX3RvaVuIn0=

6 Sec-Ch-Ua-Mobile: ?0

7 Authorization: Bearer eyJhbGciOiJSUzIiImP0aS16Ik1UNTRhVGc0TkRnd01EQxdRG95W1RFMF1qSKhZakkzIiwdh1wIjois1dUIn0.yEjzdW1o1I0MmRzmDhmZ1mHG1jTQy0Dgt0TdhCM0zj102TB10TQ5ZwylCJhdM0Q1oi1jYMQY2xP5W0i1chJpBmpGx1ijoi1HTjkZmQ4zawYzjRiY100j4Ltk3Y7AtHz1yNGUwZtk00Wm1iwiYXV0aF9wAk11ijoxHjgx0dg0DwAhDA0LcJpc3Mio1JodRhzcpc1IwvcGhpbc1wcy5b21cl2NhZc1inJbj30c1y16WjyGvuaQ1Xsw1Zhwi1ojHjg0Dg2HjAnLcPjYX0j0je20DE04MAd1lgtR0HTLWVEgi0N1Y2xh1alIj1p71khPT1hTUV1Sj1n1zRjY21IYTctZ0U3250M0DBaThkYgtZG4YVmVjZgQK0G5JmUWV1N7C16IjZtjRj1jRj1G5U5D11zJ9LcjgdQk1i1jWfkeInTrN1le5E23dNREF3Tk1rvevPURTBDz4WjMyIsIm1JdGhvcm10aVw1Ijoi09001VH

Response

Pretty Raw Hex Render

1 HTTP/1.1 301 Moved Permanently

2 Date: Wed, 19 Apr 2023 06:14:13 GMT

3 Content-Length: 0

4 Connection: close

5 Location:
https://cad-api-gateway-int.us-east.philips-healthsuite.com/phr?subject=12fdf8ff-f4bb-4208-97a0-3224e0e949ef&_sort=-effectiveDateTime&_count=1&category=ehi-sector

6 Server: envoy

7 X-Vcap-Request-Id: b68bc997-5ce8-4aeb-5b9201ed31d1

8 Via: HTTP/1.1 m_proxy_umul

9 Via: HTTP/1.1 s_proxy_umul

10

11

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Retest Status as of 24th July 2023:

Case 1: WebApp

Screenshot of a network traffic capture tool showing a request and response for a web application.

Request:

```

1 GET / HTTP/1.1
2 Host: cad-consumer-app-int.us-east.philips-healthsuite.com
3 Cache-Control: max-age=0
4 Sec-Ch-Ua:
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199
  Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
  /webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
0 Sec-Fetch-Site: none
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-User: ?1
3 Sec-Fetch-Dest: document
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-US,en;q=0.9
6 Connection: close
7

```

Response:

```

1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, must-revalidate
3 Content-Type: text/html
4 Date: Sun, 23 Jul 2023 09:03:12 GMT
5 Etag: W/"64b503eb-a3d"
6 Last-Modified: Mon, 17 Jul 2023 09:03:39 GMT
7 Server: nginx
8 Vary: Accept-Encoding
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Vcap-Request-Id: 28cd74f5-d778-4af3-50ea-81a2236b43c8
12 X-Xss-Protection: 1; mode=block
13 Connection: Close
14 Content-Length: 2701
15
16 <!doctype html><html lang="en">
  <head>
    <meta charset="utf-8"/>
    <link rel="icon" href="/favicon.ico"/>
    <meta name="viewport" content="width=device-width,initial-scale=1,viewport-fit=cover"/>

```

Allowed HTTPS Fallback

Case 2: WebServices

Refer the [Video POC](#)

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



7.12 Webapp/WebServices: Server Banner Disclosure

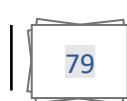
| | |
|---------------------------------|---|
| Vulnerability Title | Server Banner Disclosure |
| Vulnerability Category | A5 Security Misconfiguration |
| Severity | Low |
| CVSS V3 Calculation | CVSS Base Score: 3.1 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N |
| Description | <p>Vulnerability Description: During the security assessment, it was found that the application discloses the application server details including the version in the HTTP response. Targeted attacks can be launched against the server based on the exploits it is having. It was observed that the server nginx 1.22.1 is being used.</p> <p>Retest (17/April/2023): Server information is still getting disclosed. It was observed that nginx 1.24.0 and envoy are used. Nginx 1.24.0 has a known vulnerability "Access Restriction Bypass".</p> <p>Refer: https://snyk.io/test/docker/nginx%3Astable</p> <p>Retest as of 24-July-2023: The issue is Fixed.</p> <p>Exploitability Rational: Web server fingerprinting is a critical task for the penetration tester. Knowing the version and type of a running web server allows testers to determine known vulnerabilities and the appropriate exploits to use during testing and those are available on internet.</p> <p>Impact Rational: Targeted attacks can be launched against the server based on the exploits it is having.</p> |
| Affected Systems/IP Address/URL | <p>WebApp: https://cad-cardiovital-app-int.us-east.philips-healthsuite.com</p> <p>https://cad-consumer-app-int.us-east.philips-healthsuite.com</p> <p>https://cad-api-gateway-int.us-east.philips-healthsuite.com</p> <p>WebService Endpoint: https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report</p> |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | |
|-----------------------|--|
| Recommendation | It is recommended to use custom banner for server by hiding all sensitive information from banner. |
| Status | Closed |

Steps to Reproduce

The screenshot shows the Network tab of a browser developer tools interface, comparing a request and its response.

Request

Pretty Raw Hex

1 GET /signup HTTP/1.1
2 Host: cad-consumer-app-int.us-east.philips-healthsuite.com
3 Connection: keep-alive
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not %2A Brand";v="8", "chromium";v="108", "Google Chrome";v="108"
6 Sec-Ch-Ua-Mobile: "Windows"
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 chrome/108.0.0.0 Safari/537.36
10 Accept:
 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
 application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Content-Type: text/html
3 Content-Length: 836
4 Date: Thu, 08 Oct 2022 07:55:52 GMT
5 Etag: "630943d0-344"
6 Last-Modified: Wed, 07 Dec 2022 07:30:47 GMT
7 Server: nginx/1.22.1
8 X-Vcap-Request-Id: 7e304044-ef73-426c-4eba-f5f81fb26c7c
9 Content-Length: 836
10 Connection: Close
11
12 <!doctype html><html lang="en">
 <head>
 <meta charset="utf-8"/>
 <link rel="icon" href="/favicon.ico"/>
 <meta name="viewport" content="width=device-width,initial-scale=1"/>
 <meta name="theme-color" content="#000000"/>
 <meta name="description" content="Web site created using create-react-app"/>
 <link rel="apple-touch-icon" href="/Icon192.png"/>
 <link rel="manifest" href="/manifest.json"/>
 <meta name="apple-mobile-web-app-capable" content="yes"/>
 <meta name="apple-mobile-web-app-status-bar-style" content="black-translucent"/>
 <script src="/.env-config.js">
 </script>
 <title>
 Guided Health Services
 </title>
 <script defer="" src=".//static/js/main.7aaa179a.js">
 </script>
 <link href=".//static/css/main.9840817d.css" rel="stylesheet"/>
 </head>
 <body>
 <noscript>
 You need to enable JavaScript to run this app.
 </noscript>
 <div id="root">
 </div>
 </body>
</html>

Retest (17/April/2023):

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Request

Pretty Raw Hex

```
1 GET /static/media/dls_FoldoverDirection_16.def28fb054806e244918897e2cb23c6a.svg?
2 _WB_REVISION_=c141dba9e7db95c72ff27c247bdf50b HTTP/1.1
3 Host: cad-consumer-app-int.us-east.philips-healthsuite.com
4 Cookie: SESSION=2f4a4f54-be03-499b-a1c6-f7328e646d1a
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
6 Accept: /*
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: cors
9 Sec-Fetch-Dest: empty
9 Referer: https://cad-consumer-app-int.us-east.philips-healthsuite.com/service-worker.js
0 Accept-Encoding: gzip, deflate
1 Accept-Language: en-US, en;q=0.9
2 If-None-Match: "643bb59-320"
3 If-Modified-Since: Sun, 16 Apr 2023 08:44:09 GMT
4 Connection: close
5
6
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 304 Not Modified
2 Cache-Control: no-cache, must-revalidate
3 Date: Mon, 17 Apr 2023 08:58:57 GMT
4 Etag: "643bb59-320"
5 Last-Modified: Sun, 16 Apr 2023 08:44:09 GMT
6 Server: nginx/1.24.0
7 X-Content-Type-Options: nosniff
8 X-FRAME-Options: SAMEORIGIN
9 X-Vcap-Request-Id: 9135b04d-e0d2-4d6f-7298-35e9acbf094b
10 X-Xss-Protection: 1; mode=block
11 Connection: Close
12
13
```

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: cad-cardiovital-app-int.us-east.philips-healthsuite.com
3 Cookie: SESSION=b24104fe-db17-46e9-bef5-1df6d2d28f56; encryptedMessage=
4 U2FsdGVkXko18Dn2f0LBd6Wjn268/cCfX2Yn9RPEjteX2B8vPwDj0HAEL4kLkbzbTFR5dHRYvAeh7gEa7
5 8V038/F2B2jytCPm2f2qX2fwmqlb3eefK8BXkh3Y2D79JL4H4brsc734E4f04g80z0BMhKmuw31wqYoCoibz
6 k1D94FvFmts0sk3eYlquaswZlUm5b@0VgnxYTuln4YrnjvwIE7Wj08bVS1n0fck3Gu6v917gout35gMoy
7 aqu2lyUyGsnqM5x3VCJ2pAg6VQVA01hfj0lI9f9FhETRY1g1vSU3ipooTeSv7%2B810PtWHU346sSkt7y
8 jt+2BFx5Q@YtrB051x0h16KHPtTY1hbhF50m0N2FvvCKXQULzDg5BaH6y21lrDFK52kTxkxBNzBYoy
9 hU7BLdce1XlQq5840zN2B8x2fgyDH3GKxtMP@UrqbzSRAN2fLac7eb/4fsdwdH1LkrHuTaVgQ0ul
10 ua1j8aBllQk2ndlSPs7n63culeH7ia1f7xCssAvAza2IrM2FFFakhlHta6k9yID-2473SLuMrk2f64iro
11 s1u062BFf06619p61XFav/bg%2BaH937c1e1Sne9-8y2783krtAVspqplCKN2BXLHASL-z20HmWzHmDlw
12 8JWm1w4Hc42Fr044MUbxyogdMOKgXUvv-254RVMapGlaXmyhqnsCxKGfsAtUqFY2j4Cie4EUkqIRh2vQ
13 ElcmrIsG1v0tqChzNz5ly407p4HAYR0De!DfHdYeW473zc0U0HmHtY427fSLPkaptB1rVOnk6wLBfv
14 19g0sYhbbRaB40JPFle31gkQqsl1XewqyVKBlv5sdwghbm9rlApCGRKhkz1K0r3akdu7enjb18e%2Fe
15 QctPq4xFrcryj5pSVNU00iijr2kglu0hawazjsFH53921pEcQdVn1rYrQUAM065ow8HvR04Yzvatj6tOH
16 DRV51dg4q0%2F0QY3YJKAmid4M0Q32FTrKxe01t9qQp4Zf0lp/HjDts51AE0xVnbr2HFpoc
17 snc6NNMxJ61EfMCs53McA1lQqluuzFq3oUtV8F0jzT81n-BE7L166f8gb2t1LlTmzNmRod5r4Bv1%
18 2B6cqZ9awPQwrikyt498hdftjzaw7IlgUwVlVhQ126GMbh2pZG533JQ2F2E2hyQAQ49QsQlQhE9R0
19 b2Q8v0HfcBt7n2rYEPwzvqd9f66Q4ik/42B3dh11F1p1nwf5Ft28b0EnQjktVaymt2cUoIGy5mEw
20 2Bzyug9vXluflegusB2uZFTre0VV1M2odypbRewp54EpvJcvCD4Ab8o32KAf%2BrUMMA6347z8F2rVc7
21 Aq1Earh2jrcBzKHu5P1Ls178pocbdQuG0c16Cp2D4H6v05sHnQjxtGoXtWz32aGnfDrJ1%2Fzoyld
22 h2x2BwHmMlegrteeIo6jF0ewiISCDv2B1n2837R03oDy4WIBI6ssCvc1Fa0:QgxuiqjsvF8fj4BI
23 u5l5sPhPPpxdwmzLeub7bTFn2BEg1s2B111%2fJRAUoV8!ajLLXBf810Cln4Y4skVx2BwHP5ow6B5X2B
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Content-Type: text/html
4 Date: Tue, 18 Apr 2023 13:48:44 GMT
5 Etag: "643ba08-2f6"
6 Last-Modified: Sun, 16 Apr 2023 07:17:12 GMT
7 Server: nginx/1.24.0
8 X-Content-Type-Options: nosniff
9 X-FRAME-Options: SAMEORIGIN
10 X-Vcap-Request-Id: c1718ad7-54f3-4810-4bf9-a2441f4659bc
11 X-Xss-Protection: 1; mode=block
12 Content-Length: 758
13 Connection: Close
14
15 <!doctype html><html lang="en">
<head>
<meta charset="utf-8"/>
<link rel="icon" href="/favicon.ico"/>
<meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,viewport-fit=cover"/>
<meta name="theme-color" content="#000000"/>
```

Retest Status as of 24th July 2023

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: cad-consumer-app-int.us-east.philips-healthsuite.com
3 Cache-Control: max-age=0
4 Sec-Ch-Ua:
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
9 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199
10 Safari/537.36
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 Sec-Fetch-Site: none
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, must-revalidate
3 Content-Type: text/html
4 Date: Sun, 23 Jul 2023 09:03:05 GMT
5 Etag: W/"24b503eb-a8d"
6 Last-Modified: Mon, 17 Jul 2023 09:03:39 GMT
7 Server: nginx
8 Vary: Accept-Encoding
9 X-Content-Type-Options: nosniff
10 X-FRAME-Options: SAMEORIGIN
11 X-Vcap-Request-Id: c6db47d1-ae5d-4de4-6a23-c6eb38f4facd
12 X-Xss-Protection: 1; mode=block
13 Connection: Close
14 Content-Length: 2701
15
16 <!doctype html><html lang="en">
<head>
<meta charset="utf-8"/>
<link rel="icon" href="/favicon.ico"/>
<meta name="viewport" content="width=device-width,initial-scale=1,viewport-fit=cover"/>
```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



The screenshot shows a browser-based API debugger interface. The top navigation bar includes 'Send' (blue), 'Cancel' (grey), and navigation icons. The target URL is 'Target: https://cad-api-gateway-int.us-east.philips-healthsuite.com'. The bottom right corner shows 'HTTP/1'.

Request

| Pretty | Raw | Hex |
|---|-----|-----|
| 1 GET /engagement/report?reportStartDate=2023-07-14T10:22:30Z&reportEndDate=2023-07-14T10:22:30Z&reportType=BEATSUserId=C8d4c7d1-67af-40be-a2dd-4e74d40a44c3 HTTP/1.1 | | |
| 2 Host: cad-api-gateway-int.us-east.philips-healthsuite.com | | |
| 3 Cookie: SESSIONID=Ob7d380a-e445-4414-b6ad-a5c161075484 | | |
| 4 Sec-CH-UA: Sec-CH-UA-Mobile: ?1 | | |
| 5 Sec-CH-UA-Platform: ?1 | | |
| 6 Authorization: Bearer | | |

Response

| Pretty | Raw | Hex | Render |
|---|-----|-----|--------|
| 1 HTTP/1.1 200 OK | | | |
| 2 Access-Control-Allow-Credentials: true | | | |
| 3 Access-Control-Allow-Origin: https://cad-consumer-app-int.us-east.philips-healthsuite.com | | | |
| 4 Access-Control-Expose-Headers: Access-Control-Allow-Origin,Content-Length,keep-alive,user-agent,Host,cache-control,content-type,content-transfer-encoding,Content-Type,Authorization,authorization,user_id,edisp-introspect-value,Token,token,Access-Control-Allow-Origin,origin,X-GHS-AUTH,api-version,* | | | |
| 5 Cache-Control: no-cache,no-store | | | |
| 6 Content-Security-Policy: default-src 'self' *.philips-healthsuite.com; | | | |
| 7 Content-Type: application/json | | | |
| 8 Date: Wed, 19 Jul 2023 05:33:59 GMT | | | |
| 9 Server: envoy | | | |
| 10 Strict-Transport-Security: max-age=63072000, includeSubDomains; S-HTTP-Upgrade: max-age=600, includeSubDomains; X-Envoy-Upstream-Time: 57 | | | |
| 11 X-Trace-Request-Id: 590a291a-c3fb-48d6-7733-f0111fa1d3e | | | |
| 12 Content-Length: 1582C | | | |
| 13 Connection: Close | | | |
| 14 | | | |
| 15 | | | |
| 16 { | | | |
| "startDate": "2023-07-14T10:22:30Z", | | | |
| "endDate": "2023-07-14T14:22:30Z", | | | |
| "name": null, | | | |
| "reportType": "BEATS", | | | |
| "age": 45, | | | |
| "gender": "male", | | | |
| "height": 171.16, | | | |
| "weight": 71.0, | | | |
| "bmi": 27.740130349945204, | | | |
| "location": null, | | | |
| "type": "BEATS", | | | |
| "user_id": "C8d4c7d1-67af-40be-a2dd-4e74d40a44c3", | | | |
| "summary": { | | | |

Inspector

| Request attributes | 2 |
|--------------------------|----|
| Request query parameters | 4 |
| Request body parameters | 0 |
| Request cookies | 1 |
| Request headers | 18 |
| Response headers | 13 |

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



7.13 Webapp/WebServices: Improper Error Handling

| | |
|---------------------------------|---|
| Vulnerability Title | Improper Error Handling |
| Vulnerability Category | A5 Security Misconfiguration |
| Severity | Low |
| CVSS V3 Calculation | CVSS Base Score: 3.4 CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N |
| Description | <p><u>Vulnerability Description</u></p> <p>Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (attacker). These messages reveal implementation details which are supposed to be hidden.</p> <p>Reference: https://owasp.org/www-community/Improper_Error_Handling</p> <p>Retest as of 24-July-2023: The issue is still Valid and not fixed.</p> <p><u>Exploitability rational</u></p> <p>An attacker should have access to the application.</p> <p><u>Impact rational</u></p> <p>By leveraging the verbose error an attacker can gain more information about the target which help in fine tuning his/her future attack.</p> |
| Affected Systems/IP Address/URL | <p>WebApp: https://cad-api-gateway-int.us-east.philips-healthsuite.com</p> <p>WebService EndPoint: https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report</p> |
| Recommendation | The application should return customized generic error messages to the user's browser. If details about the error are needed for debugging or support reasons a unique identifier may be created and displayed to the user along with the generic error message for reference. This same unique identifier can be included with the error that is logged to the server so that it can be easily correlated with the issue. |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



| | |
|--------|--|
| | References: |
| | <ul style="list-style-type: none"> https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html Improper-Error-Handling-Fix-In-JAVA Improper-Error-Handling-Fix-In-ASP.NET-Core Improper-Error-Handling-Fix-In-SpringBoot |
| Status | Open |

Steps to Reproduce:

Step 1: Configure the browser to use proxy tool such as Burp Suite.

Step 2: Capture a request containing some input fields and send it to the Repeater tool.

Step 3: Manipulate the request with certain malicious characters in the input fields and observe that there is error disclosure in the response as shown in the screenshot below:

```

Send Cancel < > Target: https://cad-api-gateway-int.us-east.philips-healthsuite.com | HTTP/1
Request
Pretty Raw Hex
1 PUT /identity/Profile/12dfdb8ff-f4bb-4208-97a0-3224e0e0949ef HTTP/1.1
2 Host: cad-api-gateway-int.us-east.philips-healthsuite.com
3 Cookie: SESSION=c3b800da-4453-4f79-94cb-9eef663d76e2
4 Content-Length: 610
5 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand");v="8"
6 Sec-Ch-Ua-Mobile: ?0
7 Authorization: Bearer eyJhbGciOiJSUzI1NiIsp0a516Ik1UWTRNVxE13T1RjME5UVtJ0RHByTmkaU1UVw1PRF15IiwidHlwI
huijoxNjgwMaijoejk5c_DPN8Ux07hw0T4Xw0IQ50Dwv1QR0ZRPx9dM6RxZfgV19zrmx0GFfu0H-D
egSnuyjAaGETB11St3d40P1LyukQx71kxH181od00w18Lxo0x2t91Qamul6cNBULo-u2sdjsz2hN1Hmno
x0nmbZ533ocDDT0vrg1vpD_MP89rXkVhA0kO1QPopGaAHVCBqJU4ayYBQv7nmxsCIB_zwuAuYR1DZ
XR-Ub2Vfo59Q_r2vrGbAPBYBwYpRk3kH-1plUYw
8 Referer: https://cad-consumer-app-int.us-east.philips-healthsuite.com/
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US, en;q=0.9
11 Connection: close
12
13 {
    "userId": "12dfdb8ff-f4bb-4208-97a0-3224e0e0949ef",
    "identityId": "ebe3de0-8839-4724-beb0-85929430a470",
    "type": "<script>alert(1)</script>",
    "description": "Consumer Profile",
    "extendedAttributes": [
        {
            "attributeName": "gender",
            "value": "male"
        }
    ]
}

```

Response

```

Pretty Raw Hex Render
8 X-Envoy-Upstream-Service-Time: 241
9 X-Vcap-Request-Id: d0779eaf-0e6d-438c-6444-e5417d2138e4
10 Content-Length: 703
11 Connection: Close
12
13 {
    "id": "1e475641-97e0-4732-9755-e8b87a627982",
    "resourceType": "OperationOutcome",
    "meta": {
        "created": "1681209564402",
        "lastUpdated": "1681209564402"
    },
    "issue": [
        {
            "severity": "ERROR",
            "code": "GENERAL_ERROR",
            "diagnostics": "Validation errors [Invalid JSON format - unexpected value: <script>alert(1)</script>] [Cannot deserialize value of type 'com.philips.igt.cad.iam.dto.type.ProfileType' from String '<script>alert(1)</script>': not one of the values accepted for Enum class: [DEFAULT, PLATFORM_ADMIN, SERVICE_CONSUMER, SERVICE_PROVIDER, CUSTODIAN, ADMIN]]\n at [Source: (io.netty.buffer.ByteBufInputStream); line: 1, column: 109] (through reference chain: com.philips.igt.cad.iam.dto.UserProfileDTO[\"type\"])]"
        }
    ]
}

```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



The screenshot shows a REST API interaction between a client and a server. The client's interface includes a 'Send' button, a gear icon, and a 'Cancel' button. The URL is set to <https://cad-api-gateway-int.us-east.philips-healthsuite.com>. The request method is 'POST', and the path is '/identity/User/aed07580-0fab-4d37-9750-69864ae0ce8c?action=ADD'. The response status is 500 Internal Server Error, with the message 'Method Not Allowed'. The response body contains JSON data with fields like 'timestamp', 'path', 'status', 'error', 'message', and 'requestId'.

Request

Target: <https://cad-api-gateway-int.us-east.philips-healthsuite.com>

POST /identity/User/aed07580-0fab-4d37-9750-69864ae0ce8c?action=ADD HTTP/1.1

Host: cad-api-gateway-int.us-east.philips-healthsuite.com

Cookie: SESSIONID=23796e18-b0fb-424b-9468-68b143bf763c

Content-Length: 94

Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"

Sec-Ch-Ua-Mobile: 20

Authorization: Bearer [REDACTED]

Request

Response

HTTP/1.1 500 Internal Server Error

Access-Control-Allow-Credentials: true

Access-Control-Allow-Origin: <https://cad-consumer-app-int.us-east.philips-healthsuite.com>

Access-Control-Expose-Headers: Accept,Accept-Encoding,Connection,Content-Length,Keep-Alive,User-Agent,Host,Cache-Control,Content-Type,Content-Transfer-Encoding,Content-Type,Authorization,Authorization,User-Id,Edip-Introspect-Value,Token,Token,Access-Control-Allow-Origin,Origin,X-GHS-AUTH,Api-Version,*

Content-Type: application/json

Date: Tue, 11 Apr 2023 06:06:01 GMT

Server: envoy

X-Envoy-Upstream-Service-Time: 315

X-Cap-Request-Id: f4bed1ca-31d3-442e-7e2e-b393fa9c0a6b

Content-Length: 194

Connection: Close

{
 "timestamp": "1681193161580",
 "path": "/User/aed07580-0fab-4d37-9750-69864ae0ce8c",
 "status": "405",
 "error": "Method Not Allowed",
 "message": "Request method 'POST' not supported",
 "requestId": "8430c1a-1"
}

On adding single quote, internal server error is shown with a detailed error message

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Retest Status as of 24th July 2023

Target: <https://cad-api-gateway-int.us-east.philips-healthsuite.com>

Request

```
Pretty Raw Hex
1 GET /phr?subject=6Cb4c7d1-67af-40be-a2dd-4674d40a4cc3&sort=-effectiveDate-time&count=1
2 Host: cad-api-gateway-int.us-east.philips-healthsuite.com
3 Cookie: SESSESSION=cdb8c7-59c2-47bc-4e025de520
4 Sec-Ch-Ua: "Not A Brand", "Chromium", "88.0.4324.104"
5 Sec-Ch-Mobile: 10
6 Authorization: Bearer eyJhbGciOiJSUzIiLjAimp0aS16Ik1UWTPUVGnsTxprMElFQTNamStTpxjeUl6STF0gbU13IixiJHlwijsLSldUIn0.eyJzdWIoiYm10Ym0hNS0CMCPxIi7towYvUttYh2C00NjwzDQyWYTQ0YMLCJhdW1o1ajjYWtCZxp2WS01ivichHpbmNpcGx1joiYm1ZLNGM32RkMjdh210MGj11Wg2GcHNDY3NGC0MGRONGHEIiwiYV0aWll1joiyNgNccsOTyQwDQyLJCjpc3M1o1jeDRhwczpcL1wvvcGhpblcvyc5jblcljZN2C1sImNjbj3lcyjEWyvvcGvuaQjKXsw1Z2Qw1joxNjg5Hse1MsQwL3jpyXQj1jg1Z0Dk3HMsMNDAs1lgtRohTLUFVvFg1oms1Tchaw1z1jptIHNPt1NUWUfS1j1nFfBjBmgtODgw2z1UNWf1lOMCtYhMj1hMsq47Yt2YhVln0sInwzXQJZC1e1j1CYtjyH2QxL7tQhCtbd12s1mNsEhkDBNfDj3yHjLc0j9Hk1jNvP0t1RjM01asBNREERWtWp0s5d31mekRxTh1jdy1i+iaFlgChcm10aWv1joxQs0u1vnrv1ifQ.CX
```

Response

```
Pretty Raw Hex Render
Accept,Accept-Encoding,Connection,Content-Length,Keep-Alive,User-Agent,Host,Cache-Control,Content-Type,Content-Transfer-Encoding,Content-Type,Authorization,Authorization,UserId,edisp-Introspect-Value,Token,Token,Access-Control-Allow-Origin,Origin,X-GHS-AUTH,api-Version,*Cache-Control: no-cache, no-storeContent-Security-Policy: default-src 'self' *.philips-healthsuite.com;X-Envoy-Upstream-Service-Time: 29Content-Type: application/json; charset=utf-8Date: Wed, 11 Jul 2023 13:41:58 GMTX-Vcap-Request-ID: 59d175d2-dae6-4b06-7066-f74d52e8a625Content-Length: 370Connection: Close
```

Inspector

- Request attributes: 2
- Request query parameters: 4
- Request body parameters: 0
- Request cookies: 1
- Request headers: 18
- Response headers: 14

Improper error handelling

Target: <https://cad-api-gateway-int.us-east.philips-healthsuite.com>

Request

```
Pretty Raw Hex JSON Web Token JSON Web Tokens
1 POST /engagement/report HTTP/1.1
2 Authorization: Bearer eyJhbGciOiJSUzIiLjAimp0aS16Ik1UWTPUVGnsTxprMElFQTNamStTpxjeUl6STF0gbU13IixiJHlwijsLSldUIn0.eyJzdWIoiYm10Ym0hNS0CMCPxIi7towYvUttYh2C00NjwzDQyWYTQ0YMLCJhdW1o1ajjYWtCZxp2WS01ivichHpbmNpcGx1joiYm1ZLNGM32RkMjdh210MGj11Wg2GcHNDY3NGC0MGRONGHEIiwiYV0aWll1joiyNgNccsOTyQwDQyLJCjpc3M1o1jeDRhwczpcL1wvvcGhpblcvyc5jblcljZN2C1sImNjbj3lcyjEWyvvcGvuaQjKXsw1Z2Qw1joxNjg5Hse1MsQwL3jpyXQj1jg1Z0Dk3HMsMNDAs1lgtRohTLUFVvFg1oms1Tchaw1z1jptIHNPt1NUWUfS1j1nFfBjBmgtODgw2z1UNWf1lOMCtYhMj1hMsq47Yt2YhVln0sInwzXQJZC1e1j1CYtjyH2QxL7tQhCtbd12s1mNsEhkDBNfDj3yHjLc0j9Hk1jNvP0t1RjM01asBNREERWtWp0s5d31mekRxTh1jdy1i+iaFlgChcm10aWv1joxQs0u1vnrv1ifQ.CX
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 400 Bad Request
2 Cache-Control: no-cache, no-store
3 Content-Security-Policy: default-src 'self' *.philips-healthsuite.com;
4 Content-Type: application/json
5 Date: Sun, 23 Jul 2023 08:39:05 GMT
6 Server: envoy
7 Strict-Transport-Security: max-age=63072000; includeSubDomains;
8 X-Envoy-Upstream-Service-Time: 11
9 X-Vcap-Request-ID: da5a0a48-37ad-4bf9-5764-fa2aff57c50
10 Content-Length: 442
11 Connection: Close
12
13 {"id": "9cd7722d-be37-463e-ala8-57d9243cca73", "resourceType": "OperationOutcome", "meta": {"created": "1690101545512", "lastUpdated": "1690101545512"}, "issue": [{"severity": "ERROR", "code": "GENERAL_ERROR", "diagnostics": "Invalid request [Invalid JSON format]. [Unrecognized token 'pcp7p8x'. : was expecting {JSON String, Number, Array, Object or token 'null', 'true' or 'false']\n at [Source: (io.netty.buffer.ByteBufInputStream); line: 1, column: 11]"}]}
```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



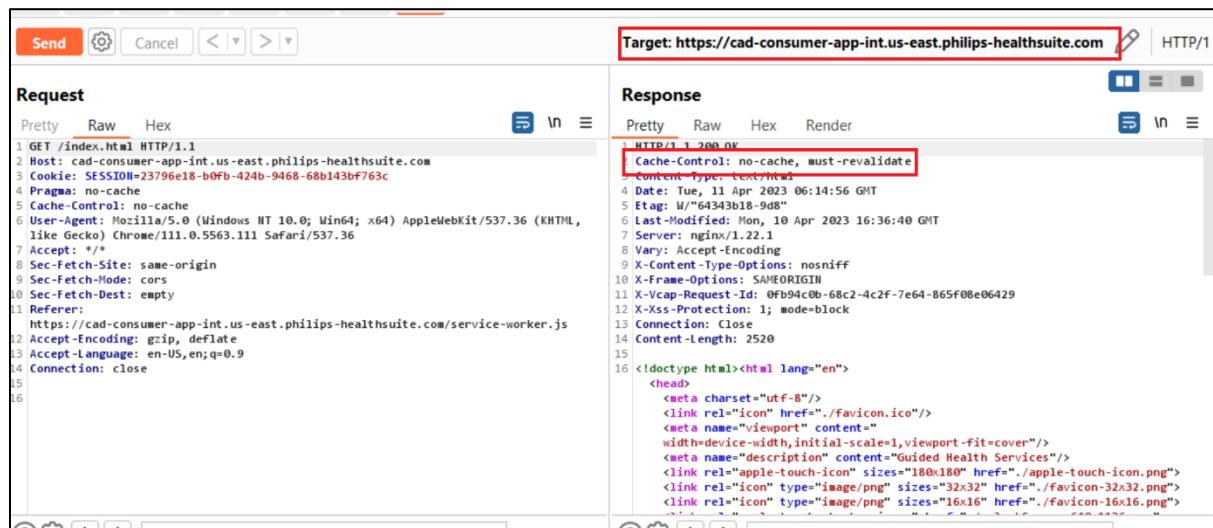
7.14 Webapp: Missing Security Headers

| | |
|-------------------------------|---|
| Vulnerability Title | Missing Security Headers |
| Vulnerability Category | A5 Security Misconfiguration |
| Severity | Low |
| CVSS V3 Calculation | CVSS Base Score: 3.9 CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:L |
| Description | <p><u>Vulnerability Description:</u></p> <p>During security assessment, we found that either the security headers are not configured properly, or security headers are missing in response. Security headers in the response can be used to increase the security of the application.</p> <p>The missing security headers are:</p> <ul style="list-style-type: none"> • Content-Security-Policy: default-src 'self' xyz.abc.company.com; • Cache-Control: no cache, no store • Strict-Transport-Security: max-age=31536000; includeSubDomains; <p>Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers</p> <p>Retest as of 24-July-2023: The issue is still Valid and not fixed, CSP not implemented.</p> <p><u>Exploitability rational</u></p> <p>Exploitability of these depends differently based on the missing headers. Like Cache-Control headers require physical access to the system. But others require user interaction to exploit this vulnerability.</p> |



| | |
|--|--|
| | Impact rational These headers provide the additional security at client side. Missing these headers may lead to sensitive information disclosure like account take over etc. |
| Affected Systems/IP Address/URL | https://cad-api-gateway-int.us-east.philips-healthsuite.com https://cad-consumer-app-int.us-east.philips-healthsuite.com |
| Recommendation | It is recommended to configure all the security headers in the response to improve your application's security. References are provided in the below links: <ul style="list-style-type: none"> https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html https://owasp.org/www-project-secure-headers/ https://help.deepsecurity.trendmicro.com/20_0/on-premise/http-security-headers.html |
| Status | Open |

Supportive Evidence:



```

Request
Pretty Raw Hex
1 GET /index.html HTTP/1.1
2 Host: cad-consumer-app-int.us-east.philips-healthsuite.com
3 Cookie: SESSION=23796e18-b0fb-424b-9468-68b143bf763c
4 Pragma: no-cache
5 Cache-Control: no-cache
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
7 Accept: /*
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: cors
10 Sec-Fetch-Dest: empty
11 Referer:
https://cad-consumer-app-int.us-east.philips-healthsuite.com/service-worker.js
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US, en;q=0.9
14 Connection: close
15
16

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, must-revalidate
3 Content-Type: text/html
4 Date: Tue, 11 Apr 2023 06:14:56 GMT
5 Etag: W/64343b18-9d8
6 Last-Modified: Mon, 10 Apr 2023 16:36:40 GMT
7 Server: nginx/1.22.1
8 Vary: Accept-Encoding
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Vcap-Request-Id: 0fb94c0b-68c2-4c2f-7e64-865f08e06429
12 X-Xss-Protection: 1; mode=block
13 Connection: Close
14 Content-Length: 2520
15
16 <!doctype html><html lang="en">
<head>
<meta charset="utf-8"/>
<link rel="icon" href="./favicon.ico"/>
<meta name="viewport" content="width=device-width,initial-scale=1,viewport-fit=cover"/>
<meta name="description" content="Guided Health Services"/>
<link rel="apple-touch-icon" sizes="180x180" href="./apple-touch-icon.png">
<link rel="icon" type="image/png" sizes="32x32" href="./favicon-32x32.png">
<link rel="icon" type="image/png" sizes="16x16" href="./favicon-16x16.png">
```

no-store directive not set, CSP not set, HSTS not set

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Request

```
Pretty Raw Hex
1 GET /phr?_sort=-occurrenceDate&resourceType=GuidanceResponse&identifier=cadphr-guid-osariskscore&_count=1&occurrenceDate&time=le2023-04-17T09:00:43.617Z
HTTP/1.1
2 Host: cad-api-gateway-int.us-east.philips-healthsuite.com
3 Cookie: SESSION=2F4a4F54-be03-499b-a1c6-f7328e646d1a
4 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
5 Sec-Ch-Ua-Mobile: ?
6 Authorization: Bearer eyJhbGciOiJSUzIiHsImp0aSI6IkI1UNTRnVGNSImp2d0lUzIiN0RG94WxpJHf16azJ2a1UhIiwiidH1wIjoi5ldUIn0_eY7zdl101zIw0Ra2DhaZ1iWnG31LToQzMDgt0TdhVc0zHjI6ZTB10TQS2WlCJ3hdqQj0iDjYmQtY2-pzH50SiwiCh0pbmPcGxL1j5o1HTkCwQ4zWt3jRiVi000j54LTk3YTATNzIyMGUz2Tk00MVzLcisInjYX0af90aW11jpoXhjgNcT2HjAx0Dc0LcJpc3M03JodRwc2pcL1iwcGhpBGlcy5jb21cl2NhZCisInjYb381cyI6dyJvcGvualQixSwd1ZmuIxjoxjgnNzI4HNDAxLcJpYXQ10j20DE3MjY2H0Es1lgtR0HtLUFVVEgi0iY2x-had1z1jprJNKPT1WUTUVSj1oIz-RjY2IIYfctZDU325000f0BmlThkY2gt2GU4VmVjZGHNz21In0sInVzZXJZC161jFyZGkOGmLWV0mHD1wC05H2eWlThjMjR1GU5H01121j9LcJqdGK10i1MVfk0T0rVejUSqlpKdIVGc:TRkef165TB2emsyMlpVMcIsImf1d0hvcm10aHvTjoiQ900U1VHRViFQ_Zc2Qcb1hB8qr21VspluxpKvu0uQdallHtUzuuKv1kDQbwv73-7Ec_ykS0tq8yXodlie_Dbc1xm3MPM2_1hm5s8SDP-kAUXX0!14G8Bp363c351h_YQNJ6L_a6H5b..._ZwhhICF199R_8TUH_61vke9719-WRkwA4UXE6bJ0lgtU-WejdlTxal0x09e6by0gth0CX46K11xFY02UsLvx7zbmwsbZhBkQ8vac7A0Z4Cd0Tksd7V3QldgYDUpoP31valjje62hHM3jaSiqCIH-UQJSXXwKgd-KsCYQ9Wl9VUF211y12qG0@utGAhJu095DX51crVocH57G
```

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36

8 Accept: application/json, text/plain, */*

9 X-Ghs-Auth:

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Credentials: true
3 Access-Control-Allow-Origin: https://cad-consumer-app-int.us-east.philips-healthsuite.com
4 Access-Control-Expose-Headers: Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,Host,cache-control,content-type,content-transfer-encoding,Content-Type,Authorization,authorization,edisp-inspect-value,Token,token,Access-Control-Allow-Origin,origin,X-GHS-AUTH,api-version,"
5 Content-Type: application/fhir+json; charset=utf-8
6 Date: Mon, 17 Apr 2023 10:17:51 GMT
7 Etag: W/"510-1e51Ehsu600UK3g+NH/8TK6xb"
8 Server: envoy
9 X-Envoy-Upstream-Service-Time: 15
10 X-Vcap-Request-Id: d87a23cc-049f-4a22-73ee-e4ea724177e7
11 Content-Length: 1296
12 Connection: Close
```

14 { "resourceType": "Bundle", "id": "d1d12945-7bca-4db3-b041-77dc0d660871", "meta": { "lastUpdated": "2023-04-17T10:17:51.102Z" }, "type": "searchset", }

Cache control, CSP, HSTS not set

Retest Status as of 24th July 2023

Request

```
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: cad-consumer-app-int.us-east.philips-healthsuite.com
3 Cache-Control: max-age=0
4 Sec-Ch-Ua:
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199
Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
0 Sec-Fetch-Site: none
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-User: ?
3 Sec-Fetch-Dest: document
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-US,en;q=0.9
6 Connection: close
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, must-revalidate
3 Content-Type: text/html
4 Date: Sun, 23 Jul 2023 09:03:05 GMT
5 Etag: W/"64b503eb-a8d"
6 Last-Modified: Mon, 17 Jul 2023 09:03:39 GMT
7 Server: nginx
8 Vary: Accept-Encoding
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Vcap-Request-Id: c6db47d1-ae5d-4de4-6a23-c6eb38f4fad
12 X-Xss-Protection: 1; mode=block
13 Connection: Close
14 Content-Length: 2701
15
16 <!doctype html><html lang="en">
<head>
<meta charset="utf-8"/>
<link rel="icon" href=".//favicon.ico"/>
<meta name="viewport" content="
```

no-store directive not set, CSP not set, HSTS not set



7.15 Webapp: Sensitive file exposed

| | |
|--|--|
| Vulnerability Title | Sensitive file exposed |
| Vulnerability Category | A5 Security Misconfiguration |
| Severity | Medium |
| CVSS V3 Calculation | CVSS Base Score: 5.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| Description | <p><u>Vulnerability Description:</u></p> <p>A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps.</p> <p>Test as of on 24 July 2023: Identified sensitive file. Issue is open.</p> <p><u>Exploitability rational</u></p> <p>To Exploit this vulnerability, attacker just need access to this webapplication and run directory bruteforce on top of the domain endpoint.</p> <p><u>Impact rational</u></p> <p>These kind fo configuration file helps attacker to make more sophisticated attacks.</p> |
| Affected Systems/IP Address/URL | https://cad-consumer-app-int.us-east.philips-healthsuite.com/.env |
| Recommendation | Restrict access to this file or remove it from the website. |
| Status | Open |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Supportive Evidence:****Test Evidence as of on 24 July 2023:**A screenshot of a terminal window titled "env". The window contains the following environment variables:

```
BUILD_PATH=../dist
REACT_APP_CAD_IAM_URL=http://localhost:8080
REACT_APP_CARDIO_VITAL_APP=http://localhost:3000
meter_definitions_base=ee7dacb4-3a10-448a-8ef0-61988dc52a8d
meter_definitions_beats_journey=6b6e5640-7dc9-42df-b7b1-a16e307a75f4
GENERATE_SOURCEMAP=false
API_VERSION = 1|
```

The terminal also shows status information at the bottom: "Ln 7, Col 16", "100%", "Unix (LF)", and "UTF-8".

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



7.16 Webapp: User Email Enumeration

| | |
|-------------------------------|--|
| Vulnerability Title | User Email Enumeration |
| Vulnerability Category | A5 Security Misconfiguration |
| Severity | Low |
| CVSS V3 Calculation | CVSS Base Score: 3.7 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N |
| Description | <p><u>Vulnerability Description:</u></p> <p>It was observed that the application signin endpoint returned verbose error messages upon authentication, indicating whether the supplied email address exists in the application.</p> <p>Test as of on 24 July 2023:</p> <p>Case 1: User Email is visible after sending the OTP. Case 2: Unregistered email mentioned in error message.</p> <p><u>Exploitability rational</u></p> <p>An attacker must be aware of or identify the pattern of email address in use to automate attacks against the authentication mechanism. Even when a email address could be identified by an attacker, it is reasonably difficult to guess the corresponding passwords using bruteforce techniques. Thus it appears highly unlikely to be exploited.</p> <p><u>Impact rational</u></p> <p>User email enumeration vulnerabilities may be abused by malicious users to identify valid email address of the application. These can be leveraged for further attacks such as password bruteforcing. Furthermore, attackers can use identified valid email address to perform Denial of Service attacks by locking out these accounts.</p> |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



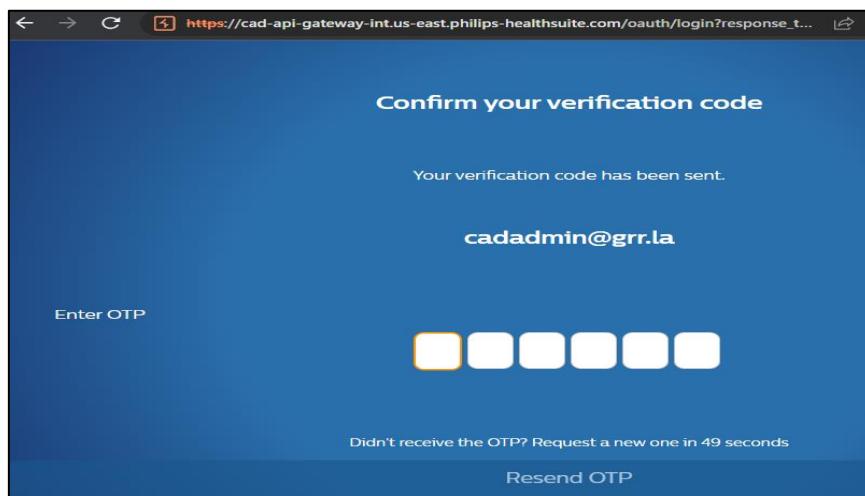
Printed copies are uncontrolled unless authenticated.



| | |
|---------------------------------|---|
| Affected Systems/IP Address/URL | https://cad-consumer-app-int.us-east.philips-healthsuite.com/signin |
| Recommendation | It is recommended to Implement the authentication mechanism such that the application displays generic error messages such as " OTP will be sent to your registered email ID". Furthermore the application should not provide other indicators in the response such as different error codes. |
| Status | Open |

Supportive Evidence:

Case 1:



a. Above screenshot shows the response for valid email address

**Case 2:**A screenshot of a web browser showing the Philips CAD Consumer App login page. The URL in the address bar is https://cad-consumer-app-int.us-east.philips-healtsuite.com/signin. The page has a blue header with the Philips logo and the text "Login or Signup" and "Great to have you. Let's get you started!". Below this is a yellow input field with the placeholder "Enter email address". Underneath the input field is an orange horizontal bar containing the text "Unregistered email id. Enroll as custodian to login with email id.". At the bottom of the page is a blue footer with the text "login with mobile number".

Enter email address

Unregistered email id. Enroll as custodian to login with email id.

login with mobile number

- b. Above screenshot shows the response for invalid email address with verbose error message
“Unregistered email ID”

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



7.17 WebServices: Misconfigured CORS

| | |
|-------------------------------|--|
| Vulnerability Title | Misconfigured CORS |
| Vulnerability Category | A5 Security Misconfiguration |
| Severity | Low |
| CVSS V3 Calculation | CVSS Base Score: 3.1 CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N |
| Description | <p>Vulnerability Description:</p> <p>During security assessment it is observed that the server is configured with an unrestricted HTML5 Cross-Origin Resource Sharing (CORS) policy. CORS defines whether resources on other domains can interact with this server. An attacker can place malicious JavaScript on his domain that can exploit the unrestrictive CORS policy to access sensitive data on this server or perform sensitive operations without the user's knowledge. Additionally, an attacker could exploit security vulnerabilities on other domains to compromise services on this server. The CORS policy relaxes the Same Origin Policy, an important security control that isolates potentially malicious resources to its respective domain name.</p> <p>If a script attempts to violate the Same Origin Policy by interacting with another domain, modern browsers can check a server's CORS policy by issuing a "pre-flight request". The browser allows the interaction only if the server responds with an Access-Control-Allow-Origin header that lists the script's domain or a wildcard match (*). A wildcard match allows interaction from any other domain, which allows any malicious content to retrieve content from this server or perform user actions.</p> <p>Test as of on 24 July 2023: Identified Misconfigured CORS. Issue is open.</p> <p>Retest as of on 28 July 2023: Issue is fixed.</p> <p>Exploitability Rational: An unrestricted CORS policy allows an attacker to access sensitive data or perform unauthorized user actions without user knowledge. Malicious JavaScript can perform these actions even if the server uses Cross Site Request Forgery tokens.</p> |

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



| | |
|---------------------------------|---|
| | <p>Impact Rational: An attacker can access sensitive data of victim. An unrestricted CORS policy allows an attacker to access sensitive data or perform unauthorized user actions without user knowledge.</p> <p>https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_(OTG-CLIENT-007)</p> |
| Affected Systems/IP Address/URL | <p>https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report</p> <p><i>Note: This is an issue with entire application endpoints. Instances are not limited to the above items. Fix should be applied across the collection.</i></p> |
| Recommendation | The Access-Control-Allow-Origin header should not be set to a wildcard match. In most cases, this header can be safely removed. If the application requires a relaxation of the Same Origin Policy, the AccessControl-Allow-Origin header should whitelist only domains that are trusted by this server. Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains. |
| Status | Closed |

Supportive Evidence:

Test Evidence as of on 24 July 2023:

Send

Cancel

< >

< >

Target: https://cad-api-gateway-int.us-east.philips-healthsuite.com
HTTP/1

| Request | Response |
|---|---|
| <pre>P GET /engagement/report?reportStartDate=2023-07-12T17:17:51Z& reportEndDate=2023-07-13T11:02:49Z&reportType=BEATS&userId= fa9e067d-42ef-44d5-96b5-f8890e803abd HTTP/1.1 2 Origin: bing.com 3 Authorization: Bearer eyJhbGciOiJSUzIiNiImsImpQasf6ik10WTRVGs1f1rReU5qWTB0VG96MVROak5XUxhaVGx oIwiwdHlwIjoiSlldU1nD_oeyJzdWl0iizjM0ZDgyNC02Nm51TrMRYUeYTYwly04NmJLYj VLODRINzgjilCJhdWQ10lJjYWotYXpx2W50iwiChJpNmNpcGx1ljoixmYzNGQ4MjotMzj0 8003mf1LWE2MDctODDi2WI1ZTgjYjca4iwiYXV0aP90aW1l1joxNjg50tK5NDt2NjQ1LCJp c3MioiJodHRwczpclLiwcGhpbGlwcy5jb21cL2Nh2CiSInNyjB1icy16MyJvcGuaWQiXSw 1ZXlwjoxNjkWMDAMXmjI2LClJyxrXqicjE2ODk5OrkUmjys1lgrR0HtLUVVVegionsiYxhaw 1zIjp7ikPEtUlojoiYwUw2TVi0WmtZTU4My0YzvhLWJhYjgtMzkyjfmNDFINGE3in0si nvZ2XJJZC1G6mJmzRkODI1MMyYzktNGzh2s1hNJA3lTg2YmV1NWU4NG13OCJ9LGJqdskj OjJNVEk071rNU9UX1oalkwl1vle1lU7mpOV1F4N1RsacIsImF1dGhvcml1aWVzIjoiQUR NSU4ifQ.UVbQIXG8h5MPdZynxb_04MrNFusU6zHouF_aYe2Ifg9eNuSa07u3spQyo6s1sk BLAWa4UueFaQ1X1wB_jtVYVYgsAKUDryD_iOAC_FnIAzXLT8QYMX0ZeHgM4nJEf7qBn-oAj jDMhMY1Wj8T_9r9sfdu399bcHv4Bcm44oInOma9VvyV1RkZegRT07Bgts1ocmOMxAGDW gfFvpL4EzfnfdTTk9i6odqs9SCFYAE2FMK9byhQULtrR8-krn871zXMV0cpTEknBjooR mCKVfim1l0tjItaLsafBneGTjXr0NB0vMluhGchka2We8B1ULx3qf0nurMm9Qg</pre> | <pre>1 HTTP/1.1 200 OK 2 Access-Control-Allow-Credentials: true 3 Access-Control-Allow-Origin: bing.com 4 Access-Control-Expose-Headers: Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent, Host,cache-control,content-type,content-transfer-encoding,Content-Type, Authorization,authorization,userid,edisp-introspect-value,Token,token,Access-Control-Allow-Origin,Origin,X-GHS-AUTH,api-version,* 5 Cache-Control: no-cache, no-store 6 Content-Security-Policy: default-src 'self' *.philips-healthsuite.com; 7 Content-Type: application/json 8 Date: Sat, 22 Jul 2023 04:43:00 GMT 9 Server: envoy 10 Strict-Transport-Security: max-age=63072000; includeSubDomains; 11 X-Envoy-Upstream-Service-Time: 31 12 X-Vcap-Request-Id: 12de7eb-87ef-4bab-7d07-eca2cb8fb3e2 13 Content-Length: 11739 14 Connection: Close 15</pre> |

Identified Misconfigured CORS (GET)

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).





Identified Misconfigured CORS (POST)

Retest Evidence as of on 28 July 2023:

Same origin is configured. Issue is fixed

PHILIPS SCOF

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



8. Tools Used

| Scope | Tools Used |
|---------------------------------------|------------------------------|
| Web Application/Web Services Security | BurpSuite Pro, NMAP, Postman |

9. Automated Tool Report



ssllscan.txt

10. Manual Test Reports and Test Case Execution

2695_CAD_GHS_SCo
E_Security_Assessmer

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.